SERIE IT PRO EN PYMES - NOTA 3 - ACCESO REMOTO

NEX IT SPECIALIST

REVISTA DE NETWORKING Y PROGRAMACIÓN

$10,80 EN TODO EL PAIS

ESPECIAL CISCO

#38

NAS FUNDAMENTALS Optimización de Storage

IP TELEPHONY Open Source

ESPECIAL NETWORKING

REDES WIRELESS Seguridad

ESCRITORIOS 3D EN LINUX

Noticias del **SOFTWARE LIBRE**

Cisco **MOBILITY**



MANAGERS EN IT
Cómo evaluan las tecnologías

DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

COORDINACIÓN EDITORIAL
- María Delia Cardenal
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

ASISTENTE COMERCIAL
- Mariana Gomez

DEPARTAMENTO DE VENTAS
- Ignacio Tellería

EDITORES TÉCNICOS
- María Delia Cardenal
- Leonardo Tomati
- Thomas Hughes
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Sabrina Furlan
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
- Ernesto Quirino
suscripciones@nexweb.com.ar

ATENCIÓN AL SUSCRIPTOR
- Fernando Ezequiel Hrzenik Sporko

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Capacitación y Salida Laboral. Necesidad de Concientizar

Nuevamente desde esta editorial queremos hacer hincapié en la necesidad que tiene Argentina de capacitar en IT. Hoy existen muchas posibilidades laborales y las universidades, gestoras naturales de recursos, apenas pueden satisfacer un pequeño porcentaje de los requerimientos.

Es importante entender que no solo expertos en programación son buscados. También hay mucha demanda de expertos en networking, seguridad informática y IT-pros.

Las empresas, asociaciones profesionales y el gobierno tienen clara esta necesidad y desde diferentes organizaciones se han implementado algunas acciones. Desde las universidades, por ejemplo, se han creado carreras cortas llamadas en general "tecnicaturas" de dos a tres años de duración. Algunos institutos terciarios tienen también ofertas de carreras breves.

Hay una alternativa, aun no muy difundida en Argentina, que tiene que ver con las certificaciones internacionales propuestas por los diferentes vendors: IBM, CISCO, Red Hat, Microsoft, Checkpoint, Oracle, SAP, entre otras. Aunque orientadas a los productos de un vendor quienes posean tal expertise y su correspondiente certificación (luego de rendir varios exámenes) son muy buscados por las empresas. Los tiempos de capacitación son relativamente cortos.

Sucede algo parecido en otros países aunque con variantes. Por ejemplo en USA hay mucho interés por parte de las universidades en promover estudios en "Computer Science". Por ello, varias campañas y acciones son implementadas. Quizás, y a pesar del esfuerzo de varias organizaciones (CESSI es un claro ejemplo), lo que falta es buscar modos de concienciar a nivel de jóvenes de secundaria sobre lo interesante que puede ser un trabajo en IT, la oferta laboral existente y los buenos salarios.

Existe una certificación de seguridad informática muy particular: CISSP. Esta es otorgada por el $(ISC)^2$ (www.isc2.org) y no está asociada a ningún vendor. Es muy difícil de obtener. En Argentina existen hoy tan solo 46 CISSP certificados. Quien hoy tenga tal certificación difícilmente no pueda hallar un excelente y muy bien remunerado trabajo.

En esta entrega de NEX #38, Ezequiel Sallis (Senior Security Specialist) nos cuenta su vivencia de ser un consultor en seguridad informática con la certificación obtenida desde hace varios años.

Los invitamos entonces a recorrer "NEX IT Specialist" #38 que incluye como siempre una colección de temas interesantes. ●

Ideas

A modo de evaluar que se hace en otros países los invitamos a que vean un video de Microsoft Research donde se promueve el estudio en Computer Science (www.nexmedia.com.ar)

NOTA DE TAPA - SECCIÓN ESPECIAL

IT



NOTAS DESTACADAS



SUMARIO - EDICIÓN #38



CentralTECH Conference Academy 2007

Con una gran concurrencia, el miércoles 27 de junio se llevó a cabo la CentralTECH Conference Academy 2007, donde acreditados expositores dieron a conocer las tecnologías y propuestas educativas de Microsoft de hoy y brindaron un panorama del futuro.

El evento comenzó pasadas las 9, con la presentación a cargo de Enrique Saggese, Senior Consultant de Microsoft Services Cono Sur, quien realizó una introducción a las tecnologías Microsoft de virtualización, ahondando en diversos conceptos de interés para los asistentes.

Cerrando la primera parte de la jornada, fue el turno del Gerente de Seguridad de Microsoft Cono Sur, Pablo Anselmo, quien cautivó a los presentes con una breve e intensa conferencia sobre seguridad, donde hizo especial hincapié en los cuidados que deben tener las empresas ante las crecientes amenazas que utilizan ingeniería social.

Al finalizar la charla, se abrieron las puertas del Salón Alejandro Casona, del Hotel Meliá, y los asistentes salieron al cómodo lounge, donde disfrutaron de un exquisito desayuno.

Tras la breve pausa, el Dr. C. Osvaldo Rodríguez, brindó un amplio panorama sobre Certificaciones Microsoft, destacando su importancia dentro del plano laboral. Además, realizó una introducción del nuevo Microsoft Official Distance Learning (MODL).

Minutos más tarde, Lucas Martinez, Gerente de Estrategia Corporativa de Microsoft Cono Sur, ofreció un amplio panorama sobre interoperabilidad y estándares abiertos, en una presentación que tituló "Conectando los mundos tecnológicos".

Pasadas las 11.30, llegó el turno de la conferencia sobre High Performance Computing (HPC), donde el Dr. Reinaldo Piz Diez le dio un toque científico a la jornada al hablar sobre la diferencia entre cálculos en paralelo y secuenciales, brindando ejemplos simples y efectivos, y sobre cómo distribuir eficientemente las tareas al utilizar computadoras de alto desempeño.

Encarando la HPC desde otro ángulo, César Ignacio Martínez Spessot, del Software Development Center de Intel Argentina, presentó oficialmente el nuevo "Intel Cluster Ready", un programa y una tecnología que ayuda a simplificar la implementación, el uso y el manejo de computadoras en clústeres proporcionando una forma estandarizada y replicable de crearlos y de ejecutar aplicaciones de alto desempeño "apenas salidas de sus cajas".

Ya sobre el final de la jornada, Ramiro Iturregui, Gerente de Socios Desarrolladores de Microsoft Cono Sur, le dio el toque "multimedia" a la conferencia, al exponer de forma interactiva su conferencia sobre "El presente y futuro de .NET".

Una vez finalizadas todas las exposiciones, llegó el momento de los sorteos, donde varios de los asistentes lograron quedarse con importantes premios, como valiosos libros sobre distintas tecnologías Microsoft, un Visual Studio 2005 y un iPod.



CALENDARIO DE EVENTOS IT EN ARGENTINA PARA 2007

Fecha		Informes
	JULIO	
13	**SAP Forum 2007** - Hotel Hilton Buenos Aires	www.sap.com/argentina/sapforum/agenda
17	**Tercer Seminario de Seguridad de la Información (Segu-Info)** - Inst. Universitario de la Policia Federal Argentina	http://www.segu-info.com.ar
	AGOSTO	
2	**Business Mobility and Convergence Conference** Hotel Hilton Buenos Aires	www.idclatin.com/argentina
14	**Intel Business Forum**	www.intel.com
21 y 22	**Congreso USUARIA 2007** - Hotel Sheraton Buenos Aires	www.usuaria.org.ar
	SEPTIEMBRE	
25	**IT Security and Business Continuity Conference**	www.idclatin.com/argentina
28	**Solid Quality Summit 2007**	http://learning.solidq.com/la

Si desea ver su evento IT publicado en esta sección, comunicarse a eventos@nexweb.com.ar

Business Mobility & Convergence Conference

El 2 de agosto se realizará la conferencia IDC Argentina Business Mobility & Convergence Conference 2007 la cual se enfocará en las tendencias del mercado de telecomunicaciones y servicios a fin disponibles para las distintas industrias y sectores del mercado.

Este foro ofrecerá a los asistentes la oportunidad de profundizar en materia de soluciones de telecomunicaciones, beneficios y ventajas asequibles para sus empresas a través de su adopción junto con los aspectos críticos en el proceso de implementación.

¿Cuánto de innovación hay en lo novedoso?

Ricardo D. Goldberger
Periodista Científico especializado
en Informática y Nuevas Tecnologías

Con la irrupción de Microsoft en el mundo del procesamiento paralelo y la grid computing, de la mano de Windows Computer Cluster Server 2008, se oficializó, para decirlo de alguna manera, la supercomputación. O, a riesgo de parecer cínico, si Microsoft incursiona en este ámbito es porque por fin pareciera que es negocio.

De más está decir que la supercomputación (etc., etc.) no es una novedad y que ya hace varios años que empresas como IBM y Sun están sacándole el jugo a este tipo de sistemas. Y no se trata sólo de aquél pionero SETI@Home que nos pedía que donemos tiempo de procesamiento para procesar –valga la redundancia– datos obtenidos de los telescopios electrónicos, o aquellos programas de United Devices (hoy uno de los grandes jugadores en el tema de la virtualización y grid computing), apoyados por Intel, que servían para hacer computación científica, cálculos moleculares y simulaciones en investigaciones de drogas contra el cáncer.

Hoy ya estamos hablando de reales aplicaciones que hacen uso del procesamiento paralelo, de grid computing. Valga como ejemplo el servicio que ofrece Mediatemple, una proveedora de hosting, que suministra 100 gigas de espacio en disco, 1 TB de ancho de banda, host para 100 sitios, hasta 1000 cuentas de e-mail por la escasa suma de 20 dólares por mes. ¿El truco? Grid computing. Y servicios de este tipo ya están en la Argentina.

A virtualizar que se acaba el mundo

Más de una vez hemos escrito –y usted ha leído notas en esta revista– acerca de las distintas variantes, virtudes y defectos, ventajas y desventajas de la virtualización. Pareciera que ahora está de moda o, para ser benévolos, pareciera que ahora está la tecnología suficiente como para que la virtualización esté al alcance de los administradores de red, gerentes de sistemas o responsables técnicos de datacenters.

Sin embargo, para ser veraces, recordemos que la virtualización es una vieja técnica que se utilizaba con éxito en aquellos antiguos mainframes que ocupaban una pared. De hecho, la virtualización que hoy conocemos, hija directa de aquélla, es prácticamente la misma que se utilizaba, aunque hayan cambiado tanto las tecnologías como las aplicaciones que la aprovechaban. Pero fundamentalmente persiste el concepto y es muy probable que haya permanecido como algo oscuro y reservado sólo a expertos si no se hubiese encontrado la manera de "bajar" la virtualización al mundo de las PCs.

Por supuesto, desde el momento en que comienza a hacerse "famosa" y a extenderse, inevitablemente surgen las aplicaciones (y no estoy hablando sólo de software) y las variantes en las que cada empresa quiere ser líder, la primera, la pionera, etc. Así, hoy hablamos no sólo de la virtualización de los sistemas operativos sino también de la virtualización de las aplicaciones o de la virtualización del almacenamiento.

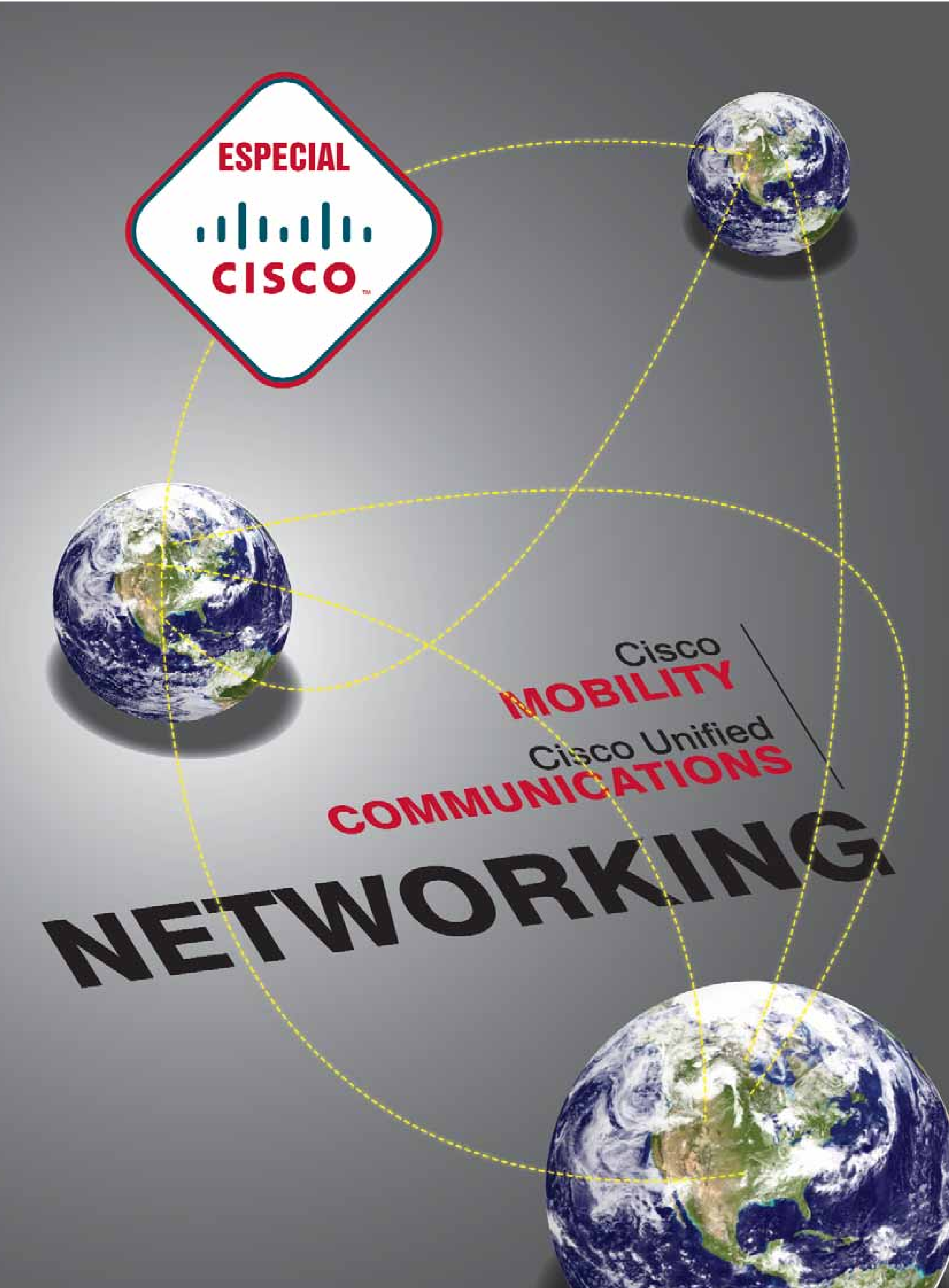
Si uno no es suficiente, que sean dos

Otro tema que también alguna vez tocamos es el de los procesadores con más de un core. Asistimos impasibles (no nos queda otro remedio) a la carrera entre Intel y AMD para ver quién saca primero el procesador con más cores de la industria. O con los cores más rápidos.

Y acá, a diferencia de los dos casos anteriores a los que nos referimos en párrafos previos, casi no hay novedades en tecnología. Sí, es cierto, ahora tenemos procesadores fabricados a 65 nanómetros y pronto vendrán a 45 y cada vez es mayor la densidad de transistores y menos el consumo de corriente y mayor la disipación de calor y...

Pero la realidad es que novedad, lo que se dice novedad, no hay. Necesitamos capacidad de procesamiento. Si no es suficiente con un procesador, ponemos dos, o le ponemos dos cores. Y si con dos no es aún suficiente, le ponemos cuatro.

En síntesis, no todo lo que reluce como novedoso es novedoso. Pero eso no significa que porque haya existido antes, no sirve o no hay que considerarlo. A la hora de proveerle a nuestro cliente de una solución, seguramente vamos a elegir una tecnología de estas. Sólo hay que estar más atento a la propia experiencia, a la actualización a través de medios serios, que a los mensajes de marketing.


ESPECIAL
CISCO
Cisco
MOBILITY
Cisco Unified
COMMUNICATIONS
NETWORKING

Surgen ideas. Se toman decisiones. Aumenta la eficiencia.
Y nace un héroe (Usted).

Como responsable de los sistemas de su empresa, usted sabe que la comunicación e interacción con los clientes es clave. Y si se realizan de una manera segura, confiable y a un precio competitivo, usted será una pieza clave en el éxito de su empresa. Con una red integrada, la colaboración y comunicación son más fáciles. Las Comunicaciones Unificadas de Cisco combinan voz, video, datos y movilidad en una red segura. Conferencias y calendarios sincronizados. Voz y video trabajando con correo electrónico. La gente puede trabajar en equipo. Donde quieran. Cuando quieran. Con o sin cables.
Y esto hace que todos trabajen bien.

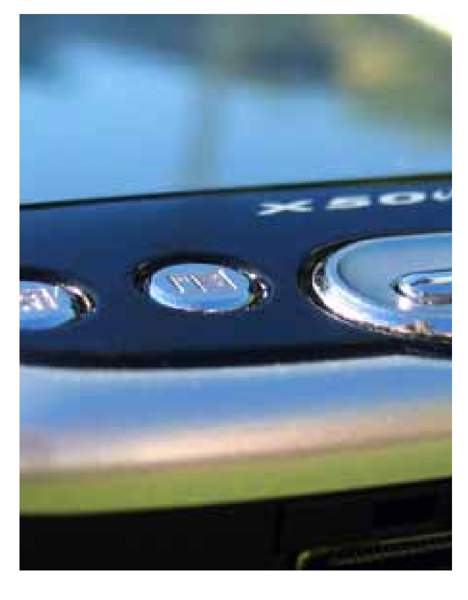
La historia continúa en www.cisco.com/offer/nextit
o llamando al 0810-444-CISCO (24726)

welcome to
the human network.



SECCIÓN ESPECIAL CISCO SYSTEMS







Cisco MOBILITY

Cisco inauguró una nueva era en la distribución de soluciones móviles enriquecidas seguras, administrables y expansibles, las que permitirán a las empresas aprovechar una cantidad de oportunidades emergentes y, al mismo tiempo, mejorar sus operaciones empresariales. Apoyando esta visión, Cisco ofrece un abanico de soluciones integradas de movilidad que ayudarán a los clientes a construir nuevas formas de conexión entre las personas, los lugares y las cosas.

Los negocios se mueven con usted

En la medida en que la inteligencia de negocios es más que una colección de aplicaciones, la movilidad empresarial se ve facilitada por un amplio ecosistema. Cisco está utilizando su extenso portafolio de productos para entregar nuevas soluciones, con el objeto de atender las necesidades de movilidad a través de diferentes industrias. Dichas Soluciones de movilidad Cisco están diseñadas sobre una red IP altamente segura, que distribuye servicios de inteligencia de conectividad tanto a Cisco como a los dispositivos y aplicaciones de sus socios. Actualmente, entre las Cisco Mobility Solutions se encuentran:

• Cisco Unified Wireless Network: provee de una plataforma segura, escalable y manejable para entregar servicios móviles.
• Cisco Mobile Solutions for Unified Communications: es una combinación entre las comunicaciones unificadas y las móviles para mejorar la efectividad de los empleados y reducir la complejidad.
• Cisco Business on the Go Solutions.
• Cisco Process Monitoring and Optimization Solutions.

Todas estas soluciones amplían el alcance de las inversiones en infraestructura de las empresas, las aplicaciones de voz y datos y los activos hacia la fuerza de trabajo móvil, donde sea que ella esté: en el campus o en una sucursal, en el hogar o trasladándose de un lugar a otro.

Insight

Insight es la habilidad que tienen los empleados de obtener información exacta para la toma de decisiones y completar el proceso de negocio sin importar en dónde se encuentren. Es más que solo acceso al e-mail o a otras herramientas colaborativas; es la información precisa para mejorar la satisfacción del cliente e interactuar con los partners.

Las tecnologías que soportan Insight incluyen:
• Tecnologías de red de cable y wireless que unen al usuario con la red empresarial para el acceso a aplicaciones y a los datos.
• Dispositivos customizados para el trabajo individual, incluyendo laptops, tablets PCs, PDAs, smart phones, teléfonos móviles y teléfonos IP.
• Soluciones de seguridad para proteger los dispositivos, la información y la red corporativa incluyendo VPN, antivirus, firewall, dispositivos NAC y la detección de intrusos.

Collaboration

Collaboration es más que la simple búsqueda de un colega, de un partner o de un cliente por teléfono, e-mail, IM o mensaje de texto. Efectivamente collaboration quiere decir buscar a la persona, no el dispositivo, de forma rápida y simple para acelerar la comunicación y la toma de decisiones.
Las tecnologías que soportan collaboration incluyen:
• Soluciones de Comunicaciones Unificadas extendidas a soluciones móviles, incluyendo smart phones o teléfonos IP wireless, como también teléfonos IP desktop.
• Aplicaciones como e-mail, voicemail, mensajes instantáneos o de texto.

FOTO: http://www.sxc.hu/ - Steve Woods - Stefanie L. - Mark Iafrate - Nathan Green / http://www.cisco.com

• La capacidad de entender quién está disponible y si desea ser contactado por teléfono, e-mail, IM o mensaje de texto.
• Capacidad de realizar audio y video conferencias que le da la posibilidad a sus usuarios de compartir documentos.

Awareness

Awareness permite la visibilidad entre los recursos y las personas claves que necesitan completar el proceso de trabajo y cumplir con los compromisos de los clientes. Conectar a la red a estos valiosos recursos deja en claro su locación y estatus, reduce el tiempo de búsqueda y los costos, y mejora la satisfacción tanto del cliente como del empleado.

La tecnología que soporta awareness incluye:
• LANs Wireless que permiten el rastreo de dispositivos móviles y de personas en un edificio.
• Etiquetas de RFID activas y pasivas que reportan el movimiento y la condición de los recursos, incluyendo temperatura, humedad, vibración y disponibilidad.

Beneficios para el negocio

Mejora la productividad, la colaboración y la respuesta

El aumento de la globalización y de la demanda de inmediatez por parte de los clientes está llevando a las organizaciones a usar la movilidad para obtener una ventaja comercial.

Las redes wireless son un componente principal de las soluciones de movilidad, ayudando a transformar los tiempos muertos en tiempo de productividad en un entorno empresarial.

Las redes wireless permiten tener acceso a personas, aplicaciones y recursos de la red en tiempo real. Los proveedores de servicios reconocen un aumento en la demanda y es por esto que están ofreciendo un nuevo e innovador servicio wireless.

Mientras las redes de alta velocidad de los municipios y las zonas públicas se expandan, una experiencia más rica estará disponible para los trabajadores móviles, aunque estén en el sistema de transporte o en un café, restaurante u hotel de la zona.

Los beneficios de la conectividad wireless se pueden ver en diferentes organizaciones de diversas industrias:

Educación: las redes wireless permite que los colegios provean de un alto rango de aplicaciones sin la necesidad de modificar el cableado, brindando a los alumnos y al personal beneficios tales como e-learning, comunicaciones de voz y acceso a Internet de banda ancha para mejorar el aprendizaje, la administración y la investigación.

Servicios financieros: las firmas de servicios financieros le brindan a los empleados móviles la posibilidad de tener un acceso instantáneo a las tendencias de la industria, datos de los clientes, e información financiera que ayuda a mejorar el servicio a los clientes y entregar de forma más rápida y eficiente productos y servicios.

Gobierno: las agencias pueden brindar acceso ininterrumpido a información crucial, logrando responder de forma más rápida y eficiente ante una crisis o las operaciones del día a día.

Salud: se puede acceder a la información del paciente en tiempo real o a su historia clínica para tomar rápidamente decisiones más precisas.

Industria: el acceso wireless a la cadena de provisiones permite que los empleados compartan información en tiempo real y mejoren los tiempos de producción.

Transporte: aerolíneas, ferrocarriles, firmas de camiones comerciales y otros negocios están utilizando redes wireless para permitirle a sus empleados una mayor movilidad. LANs wireless mejoran la eficiencia del transporte y almacenaje a través de la automatización, lo que mejora el servicio al cliente y la seguridad.







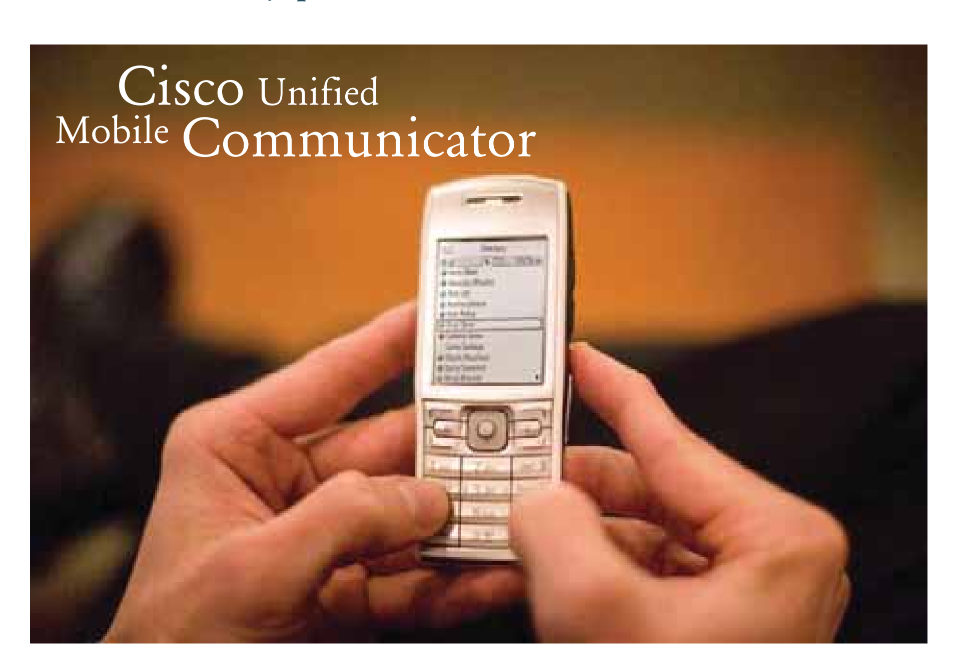
CISCO

Comunicaciones UNIFICADAS con Cisco

Conozca los productos y aplicaciones que permiten a las organizaciones utilizar su red como una plataforma para tener colaboración empresarial más efectiva y personalizada.

Hoy en día, las empresas deben lidiar con un complejo ambiente de comunicaciones que incluyen diversos métodos. Empleados, partners de negocios y los clientes se comunican entre ellos a través de una infinita combinación que incluye la comunicación por cable, wireless y por teléfonos móviles; mensajes de voz; e-mail; fax; clientes móviles; y conferencias multimedias. Pero la mayoría de las veces estas herramientas no son explotadas al máximo, obteniendo como resultado una sobrecarga de la información y poca agilidad lo que atrasa la toma de decisiones, lentifica el proceso, aleja a los clientes y reduce la productividad.

Las soluciones de comunicaciones IP han probado su habilidad de ayudar a las empresas a solucionar estos problemas, volviendo más eficiente el proceso de negocio y reduciendo los costos. Por años, las compañías han utilizado los beneficios de las comunicaciones de voz, data y video a través de una infraestructura IP en común. En la actualidad, con los productos de voz, video y comunicaciones IP del sistema de Unified Communications de Cisco, estos beneficios son mejores que nunca, logrando una mejor rentabilidad, ser más competitivos y mejorar las relaciones con los clientes.



El sistema de Comunicaciones Unificadas de Cisco 6.0 es parte de una solución integrada que incluye infraestructura de red, seguridad, movilidad, administración de red y servicios del ciclo de vida. Las Comunicaciones Unificadas de Cisco ofrecen un despliegue flexible y opciones de administración por parte de asesores, paquetes de financiamiento de clientes finales y socios, y aplicaciones de comunicaciones de terceros.

Movilidad

- El **Cisco Unified Mobile Communicator** ofrece a los empleados acceso a las comunicaciones unificadas empresariales desde teléfonos celulares y teléfonos inteligentes, usando una interfase gráfica intuitiva. El Cisco Unified Mobile Communicator permite acceso a directorios empresariales que permiten presencia, enviando mensajes de texto seguros, viendo mensajes de correo de voz empresarial y de correo electrónico desde Cisco Unity, y seleccionando mensajes individuales para escucharlos más de una vez. También permite el acceso a listas de llamadas empresariales para comunicaciones más efectivas desde un dispositivo móvil. El Cisco Unified Mobile Communicator trabaja en diferentes dispositivos de mano, en sistemas operativos móviles clave y en redes móviles múltiples, permitien-

FOTO: http://www.cisco.com

do factores de preferencias corporativas o personales tales como costo y cubrimiento.
- **El Teléfono IP Inalámbrico Unificado de Cisco 7921G** mejora la voz sobre comunicaciones LAN inalámbricas en las organizaciones y soporta los estándares 802.11 a/b/g inalámbricos. Este teléfono nuevo complementa el Teléfono IP Unificado de Cisco 7920. Al ser uno de los primeros teléfonos IP en soportar el estándar 802.11 "a", ofrece teclas dedicadas para silencio, volumen y aplicaciones como "push to talk", y una estación de carga con parlantes integrados. Este teléfono incorpora Cisco Compatible Extensions (CCX) versión 4, la cual ofrece capacidades de Calidad del Servicio (QoS) para asegurar una experiencia de alta calidad.

Empresas Pequeñas y Medianas

- El **Cisco Unified Communications Manager Business Edition** combina aplicaciones de Comunicaciones Unificadas claves para empresas medianas (100-500 empleados) en una sola plataforma. Las capacidades telefónicas son entregadas por el Cisco Unified Communications Manager 6.0, conocido anteriormente como Cisco Unified CallManager. La solución es fácil de instalar y administrar y ofrece opciones de despliegue flexible para el crecimiento. Entrega un paquete completo de funcionalidades de comunicaciones de voz y video; capacidades de número empresarial con Cisco Unified Mobility, mensajería integrada Cisco Unity Connection 2.0 y servicios de presencia. También actúa como base para más capacidades de Comunicaciones Unificadas, tales como Cisco Unified MeetingPlace y Cisco Unified IP Contact Center.
- Con el fin de satisfacer todo el rango de requerimientos para centros de contacto pequeños y medianos, Cisco está anunciando nuevas capacidades de múltiples canales y de optimización de la fuerza de trabajo para el Cisco Unified Contact Center Express. Para mejorar la satisfacción del cliente en requerimientos iniciados vía correo electrónico o web, el **Cisco Unified Web Interaction Manager** y **Cisco Unified E-Mail Interaction Manager** ofrecen una interfase de agente común diseñada para mejorar la productividad y ofrecen acceso fácil a una base de conocimiento compartida y la historia del cliente. Cisco Unified Workforce Optimization combina la administración y las herramientas de calidad de administración para ayudar a los supervisores a optimizar el desempeño del equipo para una mejor lealtad de parte del cliente.

Colaboración

- Capacidades de conferencia web basadas en flash con el **Cisco Unified MeetingPlace 6.0** ofrecen una experiencia de usuario optimizada con soporte de aplicaciones mejoradas y una solución y ambiente de usuario para conferencia web, de video y audio más efectiva y simple. Debido a que está basada en estándares abiertos y construido en la red, el Cisco Unified MeetingPlace 6.0 ayuda a permitir ahorro de costos, seguridad e integración de aplicación.
- El **Cisco Unity 5.0** introduce nuevas funcionalidades que mejoran la productividad, y permiten a los usuarios escuchar y responder mensajes en la medida en que son grabados, operación de manos libres con reconocimiento de voz y la habilidad de ver, buscar y emitir mensajes en la pantalla de un Teléfono IP Unificado de Cisco. Además, con Cisco Unity 5.0, todos los mensajes pueden ser encriptados en el sistema para obtener mayor seguridad. La habilidad para establecer la configuración de expiración de mensaje como parte de la mensajería segura ayuda a las organizaciones a prevenir que mensajes confidenciales sean enviados por fuera de la compañía.

Iniciativas de Servicios

Al utilizar el concepto de Servicios de Ciclo de Vida, Cisco y sus socios ofrecen un portafolio amplio de servicios de extremo-a-extremo para soportar el sistema de Comunicaciones Unificadas de Cisco. Estos servicios están basados en metodologías probadas para desplegar, operar y optimizar soluciones de comunicaciones IP.
Una planeación inicial y servicios de diseño, por ejemplo, pueden ayudar a acelerar un despliegue exitoso. Operar servicios incrementa la eficiencia operativa, entregando acceso inmediato a información vital, soporte técnico, incluyendo opciones para una administración remota. Optimizar servicios mejora el desempeño de la solución. Cisco y sus socios ofrecen un servicio y soporte de nivel de sistema que pueden ayudar a crear y mantener una red fiable y convergente que satisface las necesidades empresariales. El sistema de Comunicaciones Unificadas de Cisco 6.0 ayuda a que las empresas puedan sobresalir en el mundo de hoy al darles la agilidad que necesitan para innovar continuamente y adaptarse rápidamente.
Al usar la red como una plataforma segura para todas las comunicaciones – voz, video, datos, seguridad, movilidad – la red se transforma en una "red humana" donde la empresa se mueve con los empleados, la seguridad se encuentra en todas partes, y la información está siempre disponible, cuándo y dónde se necesite. ●

El **Sistema de Comunicaciones Empresariales Inteligente de Cisco** es un nuevo portafolio de productos de conectividad de voz y datos, diseñados y soportados por Cisco para extender las Comunicaciones Unificadas a clientes empresariales medianos y pequeños.
Está diseñado específicamente para responder a las necesidades y los presupuestos de empresas pequeñas (de 50 empleados o menos). El sistema ayuda a permitir un mayor número de comunicaciones más efectivas y eficientes con clientes, socios y empleados.
Dentro de este sistema encontramos por ejemplo el Cisco Unified Communications 500 Series, una solución de comunicaciones unificadas, todo en uno, que integra voz, datos, video, seguridad y tecnología inalámbrica en una sola plataforma para ayudar a entregar administración con aplicaciones empresariales existentes.



Los socios del canal en Mercados Emergentes que están buscando mejorar su rentabilidad, ser más competitivos y mejorar las relaciones con sus clientes, pueden entregar una manera fácil de vender, desplegar y servir a sus clientes al tomar ventaja de las tecnologías de Cisco, diseñadas para trabajar en conjunto y simplificando y monitoreando la red empresarial de pequeñas y medianas empresas, y a la vez, entregando oportunidades para nuevos ofrecimientos de servicio con nuevas corrientes de ingresos.
Las empresas pequeñas y medianas están buscando productos con precios apropiados y servicios que respondan a sus necesidades crecientes de comunicación. Con la nueva solución Cisco Unified Communications 500 se da la posibilidad de entregarle a este tipo de compañías en la región capacidades de comunicación de clase empresarial a un precio accesible.

Centro de Atención a Clientes.

Con una red integrada sus clientes reciben el cuidado y servicio que merecen, las 24 horas del día, los 7 días de la semana. La solución Cisco Unified Contact Center se integra a la red. El crecimiento es perfecto. En cualquier momento, en forma virtual y eficiente. Las llamadas y requerimientos de los clientes se analizan, se atienden de acuerdo a las prioridades y se procesan inmediatamente, con seguridad.
Así, los clientes no sólo quedan sonriendo, regresan!

La historia continúa en www.cisco.com.ar
o llamando al 0810-444-CISCO (24726).

welcome to
the human network.





FOTO: http://www.sxc.hu/ - Jayesh Nair

Redes Wireless
Seguridad

La seguridad en la redes wireless ha evolucionado muy favorablemente en los últimos años pasando de redes inseguras, con el uso de WEP, a redes impenetrables, gracias al protocolo 802.11i (WAP2).

Fernando A. Luciague
Ingeniero Electrónico (UBA)



En esta edición veremos cómo fue la evolución de la seguridad en las redes wireless y porqué tuvo un principio con dificultades. También veremos cómo podemos hacer nuestra red más segura y cuáles son los ataques más conocidos.

WEP (Wireless Equivalent Privacy) en 802.11b

Cuando se definió el protocolo 802.11b se pensó en la seguridad y se definió lo que se conoce como **WEP** (Wired Equivalent Privacy). WEP es un sistema de cifrado que se incluyó en el estándar 802.11b, tanto para el cifrado de datos como para la autenticación con la posibilidad de poder realizarlo por separado o en conjunto. Como algoritmo de cifrado se optó por el conocido **RC4**, que en un principio se pensó que era suficiente, pero el uso de este código tiene algunos problemas. El primero es que el código de RC4 está disponible en Internet y el segundo es que al estar disponible para cualquiera, hay muchas aplicaciones creadas por hackers que rompen el código de RC4 usando lo que se llama *weak keys*. Para entender un poco más de porqué WEP es vulnerable por RC4 hay que entender cómo funciona RC4 y el proceso de cifrado. Lo primero que hay que saber es que RC4 utiliza la función XOR en combinación con la llave secreta para cifrar los datos. La llave para cifrar que se utiliza en WEP es una combinación de dos elementos, uno estático y uno dinámico. El elemento estático es la llave secreta, valor alfanumérico de 40 ó 104 bits. El elemento dinámico coincido como IV (Initialization Vector) es de 24 bits y este valor se le adhiere al valor estático formando la llave WEP de 64 ó 128 bits.

Como se ve en la figura 1, el **plaintext** (texto plano) que son los datos sin encriptar, se pasa por un algoritmo llamado **Integrity Algorithm** que genera un **ICV** (Integrity Check Value) que luego se le adhiere al plaintext. Por otro lado se genera un IV y junto con la **secret key** (llave secreta) se pasa por el algoritmo de RC4 dando un valor conocido como "*C value*" que luego se inserta en un **PRNG** (Pseudorandom number generator) que produce la llave de cifrado. Luego estos dos resultados pasan por una función XOR y da como resultado el **ciphertext** (texto cifrado) que a este se le adhiere el IV. Cada vez que ocurre este proceso los IV van cambiando.

En principio parece bastante seguro, pero el problema ocurre en el uso de los IV, como se mencionó anteriormente el tamaño de los IV es de 24 bits y esto nos da una cantidad de 2^{24} = 16777216 IVs, que parece mucho pero en una red muy ocupada los IVs se repiten muy rápido y con el uso de aplicaciones llamados packets sniffers (husmeador de paquetes) un atacante puede capturar suficientes IVs con una PC. Cuando se logra obtener

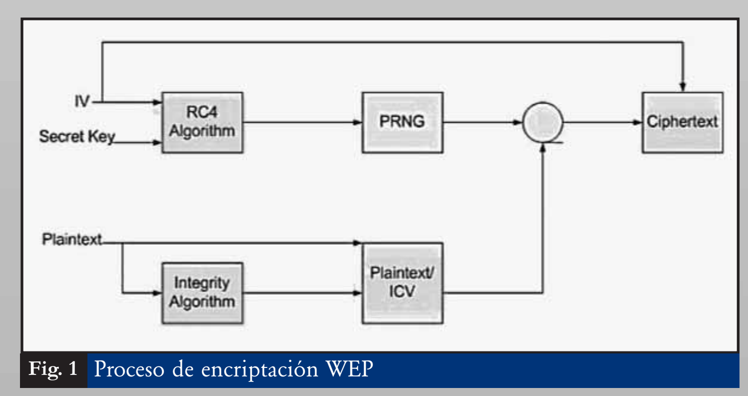


Fig. 1 Proceso de encriptación WEP

IVs duplicados y con el uso de aplicaciones llamadas WEP crackers (Rompedor de WEP), se puede obtener la clave WEP y con esto adiós a nuestra seguridad. Este proceso hoy en día dura solo unos minutos. Se puede concluir que existen dos problemas en este proceso de cifrado, el primero es el tamaño de los IVs y el segundo es enviar los IVs sin cifrar. Entonces algo para tener en cuenta es que la culpa no es del RC4 sino los IVs.

Usos de Filtros (Filtering) para una red más segura

Para poder hacer más segura una red WLAN se utilizan filtros, estos pueden ser:

- **SSID**
- **MAC Address**
- **Protocolos**

Los filtros de **SSID** son utilizados para que no encuentren nuestra red, hay que recordar que el SSID es el nombre de la red, entonces si alguien quiere atacar a una red en particular y esta no tiene el filtro de SSID habilitado será muy fácil encontrarla. Como se explicó en la edición #36, el SSID se envía en la trama beacon y esta trama se envía en forma de broadcast y por lo tanto el SSID. Pero se puede habilitar que no se envíe el SSID y con ello lograr que no encuentren nuestra red, a esto se le llama generalmente un "*closed system*". También es importante cambiar el nombre de default del **AP** (access Point) ya que cada fabricante tiene el suyo y son muy conocidos, y tampoco usar un nombre muy obvio, como el nombre de nuestra empresa.

Filtro por **MAC Address**, en este caso el AP se configura para permitir o negar la asociación basado en la MAC address de una estación. Esto en principio también parece bastante seguro, pero el problema está en que la MAC address no se envía cifrada entonces se puede capturar las MAC address fuente y destino, luego teniendo esta información la persona que desea entrar en la red solo tiene que cambiar la MAC address de su placa de red wireless.

Por último, el filtro por **protocolos** es utilizado para permitir o negar el uso de ciertos protocolos como FTP, HTTP, HTTPS, DNS, SMTP, POP3, Telnet. Este filtro le da a la red cierta seguridad como así también control del uso da ancho de banda.

STA – Station – device accessing the network
AP - Access Point
AS - Authentication Server

Fig. 3 Autenticación vía RADIUS Server

Ataques a una red WLAN

Los ataques a una red WLAN pueden dividirse en cuatro categorías:

- **Pasivos**
- **Activos**
- **Jamming**
- **Man in the middle**

Se habla de ataques **pasivos** porque el atacante utiliza un analizador de protocolos y captura paquetes de una red y sin dejar rastro se lleva mucha información que puede estar cifrada o no. Si está cifrada como ya vimos con la suficiente información y con el software adecuado se puede obtener la clave WEP. Luego con la clave puede realizar un ataque **activo** que es entrar en nuestra red y robar o destruir información valiosa, usar el acceso a Internet, etc.

El ataque **jamming** no es muy común, ocurre cuando el atacante utiliza un generador de alta potencia de señales RF y con esta señal logra interferir nuestra señal y dejar sin conexión nuestra WLAN. Pero no obtiene ningún tipo de información, solo se pierde la conexión por un determinado tiempo. Este tipo de ataque solo causa una perdida en la productividad de la empresa.

Man in the middle se da cuando un intruso que tiene la capacidad de leer, insertar y modificar los datos que se envían entre dos partes de una red pero sin que estos se den cuenta de ello. En la figura 2 se ilustra man in the middle.

Este tipo de ataque permite subataques. Estos pueden ser el secuestro de una sesión que se realiza mediante la usurpación de la dirección MAC de un usuario legítimo. Otro tipo de ataque más permanente es la corrupción de la memoria caché ARP, esto se logra debido a que el protocolo ARP no tiene diagramas de estado y cualquier PC puede aceptar un ARP response sin haber emitido un ARP request. El protocolo ARP trabaja a nivel de enlace de datos del modelo OSI, entonces este ataque solo puede ser realizado en la parte de la red que queda antes del primer router, o sea a nivel de capa 2. Esto afecta a las redes WLAN como LAN. Una forma de prevenir este tipo de ataque es crear la tabla ARP en forma manual y filtrar el tráfico ARP, aunque administrativamente puede resulta engorroso.

Alternativas al WEP

Tener una clave WEP asignada en forma estática no provee seguridad alguna como ya se ha demostrado, entonces lo que se necesita es una asignación dinámica de la clave para una estación (STA) y un AP, que puede realizarse por sesión o paquetes. Pero esto solo no es suficiente, también se necesita un método que no permita que usuarios no autorizados puedan acceder a la red protegida. Para este propósito se utiliza el estándar **802.1x** que permite la autenticación y autorización de dispositivos conectados a una LAN o a una WLAN. Para poder realizar la distribución dinámica de claves y a su vez tener un sistema robusto para la autentificación y autorización se utiliza un servidor **RADIUS** (Remote Authentication Dial In User Service) y protocolo EAP (Extensible Authentication Protocol) que puede elegir entre varios protocolos de autentificación. Su funcionamiento se ve en la figura 3.

El AP presta un servicio de autentificación a la estación STA comunicándose con un servidor RADIUS que valida a la STA. El protocolo EAP pertenece a la fase de autentificación pero para realizar ésta elige un protocolo de autentificación como MD5 (message Digest 5), TLS (Transport Layer Security), TTLS (tunneled Transport Layer Security).

Una alternativa al 802.1x es la utilización de VPNs (Virtual Private Network) que resultan ser más complejas para manejar que la solución 802.1x/EAP.

Si bien estas alternativas son seguras, se comenzó a pensar en un nuevo estándar que permitirá un mecanismo de seguridad invul-

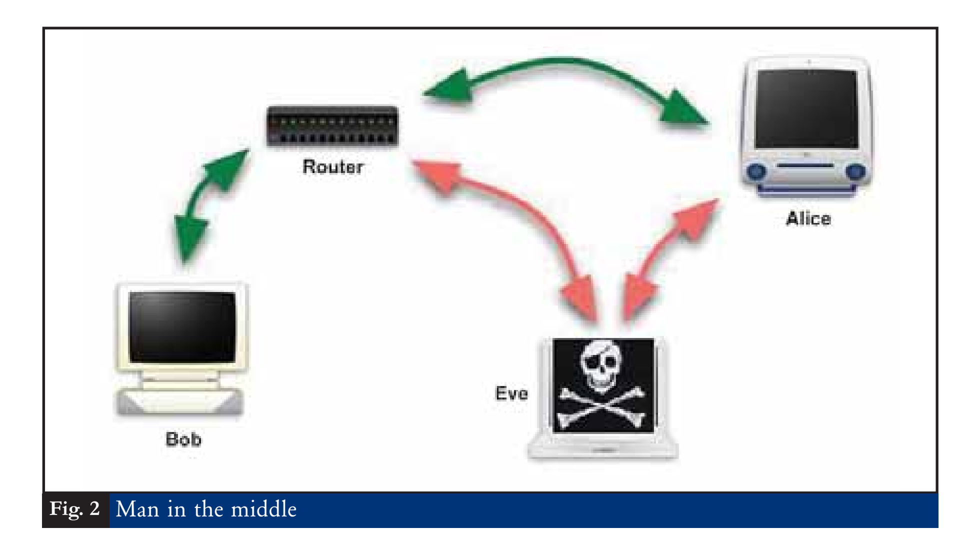


Fig. 2 Man in the middle

10 Tips
para tener una WLAN segura

1- Si es posible usar siempre WAP o WAP2 sino WEP de 128 bits.

2- No utilizar un SSID muy descriptivo de nuestra empresa.

3- Cambiar el password y la IP que vienen por default en el AP.

4- Deshabilitar el broadcast del SSID.

5- Utilizar MAC filtering sino nos resulta muy engorroso.

6- No colocar el AP cerca del perímetro del establecimiento, para evitar emanaciones de RF hacia fuera o sino utilizar antenas-panel que direccionen la radiación hacia adentro.

7- Poner firewalls en el límite entre la WLAN y la LAN.

8- Autenticar los usuarios con RADIUS.

9- Utilizar VPNs en lo posible.

10- Utilizar métodos seguros de encriptación: 802.1x/EAP-TLS, EAP-TTLS, etc.

nerable, este estándar se lo conoce como 802.11i, pero antes de que fuera aprobado la Wi-Fi Allinace propuso una solución intermedia conocida como WAP (Wi-Fi Protected Access) que solo implementa una parte del 802.11i. WPA fue diseñado para utilizar un servidor de autenticación RADIUS que distribuye claves diferentes a cada usuario, a través del protocolo 802.1x. Pero también se puede utilizar en un modo menos seguro, conocido como PSK (Pre-Shared Key) que se recomienda su uso en casas o pequeñas oficinas. La información es cifrada utilizando el algoritmo RC4 como en WEP ya que WAP no elimina el proceso de cifrado de WEP sino que lo fortalece con una clave de 128 bits y un vector de inicialización de 48 bits. Otra mejora es la implementación del protocolo TKIP (Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Esto en combinación con un vector de inicialización (IV) mucho más grande, evita los ataques a los que es susceptible WEP.

WPA también mejora la integridad de la información cifrada, ya que el chequeo de redundancia cíclica CRC (Cyclic Redundancy Check) utilizado en WEP es inseguro porque es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje MIC (Message Integrity Code), conocido como *"Michael"*. También incluye un contador de tramas que protege a la red de ataques de repetición.

El estándar 802.11i se lo conoce como WPA2 y a diferencia de WEP y WAP este estándar utiliza el algoritmo de encriptación AES (Advanced Encryption Standard) que no ha sido objeto de ningún ataque conocido. ●

Protocolo DNS

El protocolo DNS permite relacionar los diferentes nombres de dominio con las direcciones correspondientes, para que cada una de las aplicaciones pueda comunicarse con los hosts remotos.

Miguel F. Lattanzi
Ing. en Telecomunicaciones (IUPFA)

Introducción

El protocolo DNS (Domain Name System) corresponde a la capa de aplicación, por lo tanto viaja encapsulado en un protocolo de capa 4. Recordemos que la capa cuatro es la capa de transporte del modelo de referencia OSI (Open Systems Interconnection).

El mismo puede ser encapsulado tanto sobre el protocolo UDP (User Datagram Protocol) como sobre TCP (Transmission Control Protocol), utilizando el puerto 53 para establecer la sesión de comunicación. Normalmente por convención se lo encapsula sobre UDP.

DNS se utiliza para poder mapear -realizar un mapping- los nombres de dominio a un valor dado, como por ejemplo a una dirección IP (Internet Protocol). Además del mapping a una dirección IP -lo cual se desarrolla en el presente artículo- existen otros usos; por ejemplo, los agentes de e-mail utilizan al protocolo DNS para conocer el destino o destinos de los mensajes enviados.

Un ejemplo de la funcionalidad de DNS para el mapeo de direcciones de Internet a partir de nombres de dominio sería traducir el nombre de dominio eureka.org a la dirección IP 66.215.223.30. Por medio de este protocolo el cliente (host) que se quiera comunicar con eureka.org puede conocer su dirección para establecer la comunicación, recordemos que el direccionamiento de la información se realizar por medio de las direcciones IP a través de los routers.

Vemos entonces como DNS logra resolver este problema, dado que es mucho más sencillo recordar un nombre de dominio que una dirección IP, más aún hoy que una persona promedio puede hacer uso de 20 páginas de Internet en forma frecuente, imagínese el esfuerzo necesario para recordar más de 10 direcciones IP para una persona que no trabaja con tecnologías de comunicaciones.

DNS fue creado en 1983 por Paul Mockapetris, las primeras especificaciones de funcionamiento aparecieron en las **RFC 882** y **RFC 883** del IETF (Internet Engineering Task Force). Más tarde en 1987 se publicaron dos nuevas especificaciones, la **RFC 1034** y la **RFC 1035** que establecían diversas actualizaciones y dejaban a las precedentes como obsoletas.

Estructura Funcional

DNS está soportado por un conjunto de servidores que están agrupados en orden jerárquico, siguiendo un esquema de árbol descendente. Los diferentes servidores representan los distintos espacios de nombres de dominio, los cuales a su vez se subdividen en zonas. Cada zona corresponde a un conjunto de servidores que forman un subárbol dentro del esquema general. Cada nodo dentro de la estructura guarda información relacionada con el nombre de dominio, esta información es guardad en lo que se conoce como "Resource Record". Por otro lado, cada zona tiene un servidor principal que se encarga de administrar el subárbol inferior de servidores, este servidor se conoce con el nombre de "Authoritative Name Server".

La zona principal, conocida como "Root Zone", es administrada por el conjunto de root servers que la conforman. Existen 13 de estos servidores en todo el mundo, los cuales en su conjunto conforman la entidad superior que gobierna la estructura y el funcionamiento del servicio DNS. En la figura 1 puede verse un

> "DNS se utiliza para poder mapear los nombres de dominio a un valor dado, como por ejemplo a una dirección IP"

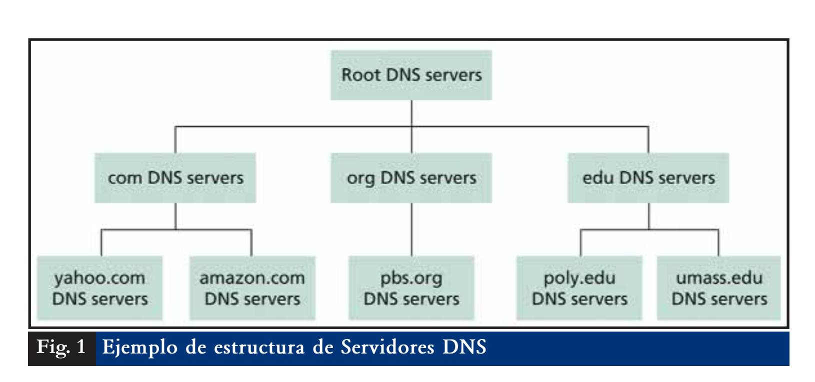


Fig. 1 Ejemplo de estructura de Servidores DNS

ejemplo de la estructura, ya mencionada, de los servidores. La figura 2 muestra la ubicación y la autoridad a la que pertenecen los 13 root servers actualmente en servicio.

Dentro de la estructura existen, además, los "Top Level Domain" (TLD) y los "Hostname". Los primeros están identificados por la etiqueta más hacia la derecha del nombre de dominio, mientras que los segundos son aquellos dominios identificados por una dirección IP, prácticamente cualquier subdominio. Tomemos el siguiente nombre de dominio para poder realizar un análisis de lo explicado: chandra.harvard.edu.

El TLD en este ejemplo es **edu**, mientras que el hostname es **chandra.harvard.edu**, identificado con la dirección IP 131.142.185.93.

Siguiendo la estructura de DNS podemos definir, a su vez, que chandra.harvard.edu es un subdominio de harvard.edu, el cual es un subdominio de edu. Cabe destacar que tanto chandra.harvard.edu como harvard.edu son hostname porque están identificados con una dirección IP en particular, pero no así el dominio edu.

Dado que la cantidad de subdominios posibles a traducir en direcciones IP es muy grande, para aumentar la eficiencia en la comunicación entre los diferentes servidores, cada uno de ellos conoce la dirección de los root servers y la de sus servidores inmediatamente inferiores. De esta manera se pueden realizar búsquedas rápidas y efectivas.

Funcionamiento

El protocolo DNS entra en funcionamiento cuando una aplicación requiere resolver un determinado nombre de dominio a una dirección IP, por ejemplo, para comunicarse con un host remoto. Los pasos a seguir son:

1- La aplicación realiza una petición, por medio de un mensaje *DNS Query*, al DNS Resolver -también llamado DNS Client-, el cual es un módulo dentro del sistema operativo. Este se encarga de resolver los nombres de dominio. Primero verifica su cache local, en donde se encuentran guardados *n* últimos resultados. Si encuentra que es capaz de responder la información solicitada, solo se encarga de responderle a la aplicación, por medio de un mensaje *DNS Reply*, para que esta pueda continuar con la comunicación.

2- En caso de no poder responder, reenvía la consulta al servidor de DNS local, perteneciente por lo general al ISP (Internet Service Provider) que esté proveyendo la conexión. Generalmente se configuran dos servidores de DNS, uno primario y otro secundario. Copiando la lógica ya utilizada, el servidor local primero realizará una búsqueda en su cache local. Si posee la información responderá con un mensaje *DNS Reply* al DNS Resolver del host. Este último agregará la información a su cache local para uso futuro y reenviará la respuesta a la aplicación que realizó la petición original.

3- De no poseer la información, el servidor de DNS local reenviará el mensaje de query a servidores de nivel superior para realizar una búsqueda más extensa, la cual finalizará con una de dos maneras posibles: con un mensaje *DNS Reply* hacia el servidor local y hacia el host; o con un mensaje de error en el caso de no poder resolver la petición original.

La figura 3 muestra un ejemplo de una búsqueda DNS, tener en cuenta que los números de la figura solo establecen el orden en el flow de la mensajería intercambiada por los diferentes nodos, no haciendo referencia a los pasos explicados anteriormente.

Existen dos tipos diferentes de mecanismos de búsqueda utilizados por el protocolo DNS y su estructura de funcionamiento, los mismos corresponden a búsquedas *Iterativa* y *Recursiva*.

Las búsquedas Iterativas son aquellas en las cuales el servidor consultado no conoce el nombre de dominio pero informa a qué servidor se debe preguntar.

Las búsquedas Recursivas son aquellas en las cuales el servidor consultado no conoce el nombre de dominio y retransmite la consulta a otro servidor, que a su vez, si no conoce el nombre de dominio consulta a un tercero, y así sucesivamente. ●

Root DNS server
Local DNS server
dns.poly.edu
TLD DNS server
Authoritative DNS server
dns.cs.umass.edu
Requesting host
cis.poly.edu
gaia.cs.umass.edu

Fig. 3 Ejemplo de consulta DNS

> "El protocolo DNS entra en funcionamiento cuando una aplicación requiere resolver un determinado nombre de dominio a una dirección IP, por ejemplo, para comunicarse con un host remoto"

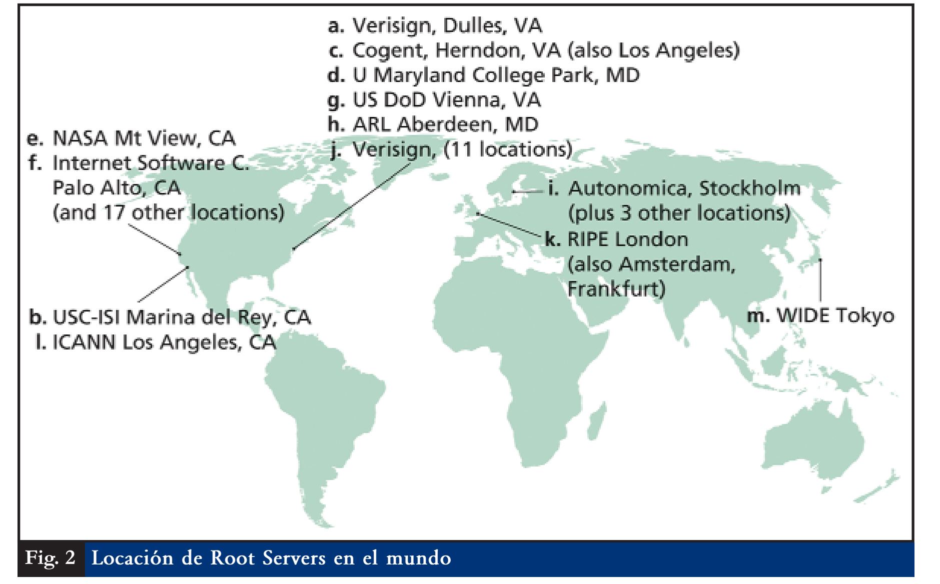


Fig. 2 Locación de Root Servers en el mundo

NAS Fundamentals

Sebastián Cesario

Dentro de las estrategias de consolidación de storage es muy común oír hablar de la estrategia de SAN, la cual permite optimizar el uso de recursos de storage al poder ser concentrados en un equipo y compartido por varios servers, lo cual trae grandes beneficios, pero todavía no es tan común en Argentina el hablar de NAS.

NAS (Network Attached Storage) tiene como particularidad principal que se basa en el manejo de archivos, en vez del manejo de bloques del cual hace uso la tecnología de SAN (Storage Area Network), permitiéndonos de este modo poder centralizar el almacenamiento de archivos a través de la LAN.

Un poco de historia

NAS nace principalmente de dos grandes grupos, SUN Microsystems por un lado, desarrollo NFS (Network File System), mientras que en paralelo Microsoft e IBM desarrollaron SMB (Server Message Block). En primera instancia, IBM usó SMB como protocolo de nombramiento y búsqueda, adaptado luego por Microsoft como protocolo de file-sharing. SMB derivó con el paso del tiempo en CIFS (Common Internet File System), protocolo usado por Windows y OS/2. Este protocolo fue pensado originalmente con una idea más orientada al acceso concurrente que a la performance. Por otro lado, NFS nace como un proyecto realizado por ingenieros de SUN, liberado al público en 1984, y adoptado posteriormente por todas las plataformas UNIX.

NFS fue pensado para poder centralizar los directorios del */home* de todos los usuarios en un único equipo y compartirlos con el resto a través del mismo. NFS fue diseñado originalmente para trabajar en UDP, a pesar de que a partir de la versión 3 adopta también el TCP, la mayor parte del tráfico utiliza UDP. NFS y CIFS ganaron popularidad a través del tiempo y, a pesar de los beneficios obtenidos, se presentan problemas a resolver como ser el hecho de que no se podía tener un solo servidor como servidor de NFS y CIFS. Esta problemática da inicio al NAS.

Funcionalidades Importantes

SNAPSHOT

Dentro de los features adicionales que proveen los equipos de NAS, vale la pena destacar el snapshot. Éste provee la capacidad de realizar copias instantáneas de un volumen en un momento en el tiempo, las cuales son almacenadas en modo de solo lectura, sin overhead de performance para mantener el volumen original y la copia online. Esta herramienta sirve, por ejemplo, para realizar backup online de un volumen, realizando una copia online del mismo y permitiendo de ese modo la continuidad de la operación. Otro uso puede ser el generar una copia de producción para hacer pruebas en un servidor de testing.

MAILBOX

Muchos de los vendors ya poseen agentes que interactúan directamente con las aplicaciones más conocidas, un ejemplo es el mailbox recovery para Exchange Server, el cual permite restaurar, por ejemplo, una casilla dentro de una base y no restaurar la base entera. Como este hay varios ejemplos de integración con aplicaciones dependiendo del vendor.

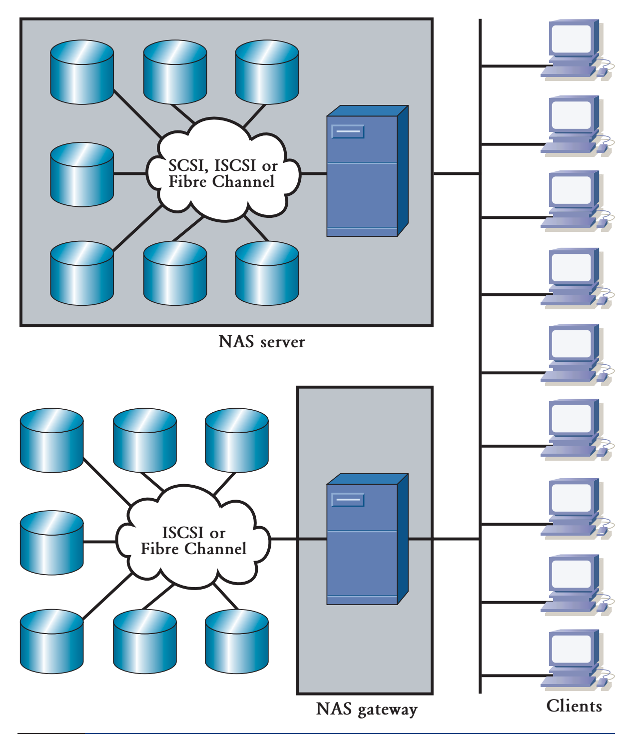


Fig.1 Diferencias entre NAS Server y NAS Gateway

Arquitectura

El concepto de NAS es simple, propone eliminar los problemas de compatibilidades entre NFS y CIFS, a la vez que permite consolidar en una caja especifica un arreglo de discos que provea redundancia, performance, administración centralizada y una estrategia que permite aprovechar y maximizar el uso de recursos de storage.

A grandes rasgos existen dos tipos de arquitectura de NAS, el NAS Server, que provee los servicios de NAS y posee la capacidad de disco embebida en la misma caja, y el NAS gateway, el cual provee los servicios a través de un equipo pero la capacidad de disco es provista a través de iSCSI o Fibre Channel.

Ventajas y usos del NAS

Los NAS gateways y servers son típicamente usados en tres grandes áreas de negocio: consolidación de datos, aplicaciones de Internet y aplicaciones de negocios. De esta manera se resuelve la complejidad del datacenter presentando un único punto de administración para los datos, reducción de costos de infraestructura, y haciendo uso de los siguientes beneficios aportados por esta tecnología:

Facilidad del startup: Los productos de NAS han sido diseñados para conectarse a la red y

Worm

Algunas empresas se ven sujetas a cumplir con determinadas regulaciones de retención de datos, la mayoría de los equipos de NAS actualmente en el mercado proveen la tecnología WORM (Write Once – Read Many), la cual posibilita cumplir con la retención de datos que no pueden ser borrados ni reescritos.

empezar a compartir archivos, el tiempo de startup es realmente corto y su configuración fácil de realizar.

Features Adicionales: Se puede hacer uso de features tales como snapshots, alta disponibilidad, volúmenes flexibles, backup centralizado, etc.

Manejo de Arreglos de Discos: Los NAS servers, permiten configurar los arreglos de discos de acuerdo a nuestros requerimientos (RAID 0, 1, 4, 5, 10, 0+1).

Escalabilidad: Los NAS servers permiten crecimiento acompañando los requerimientos de nuestro negocio, así como también hacen fácil el reemplazo y upgrade de servidores ya que los datos se encuentran separados del Server físico y solo hay que redireccionarlos.

Rapidez en la curva de aprendizaje: Los productos de NAS son lo suficientemente fáciles de usar, como para que cualquier administrador de sistemas pueda rápidamente familiarizarse con el producto.

Limitaciones del producto

NAS tiene limitaciones propias de su diseño. Así como tiene un excelente rendimiento para file sharing, hacer uso de aplicaciones I/O intensive, como bases de datos o aplicaciones de proceso de video no es recomendado ya que en algunos casos NAS no provee la performance adecuada para las mismas.

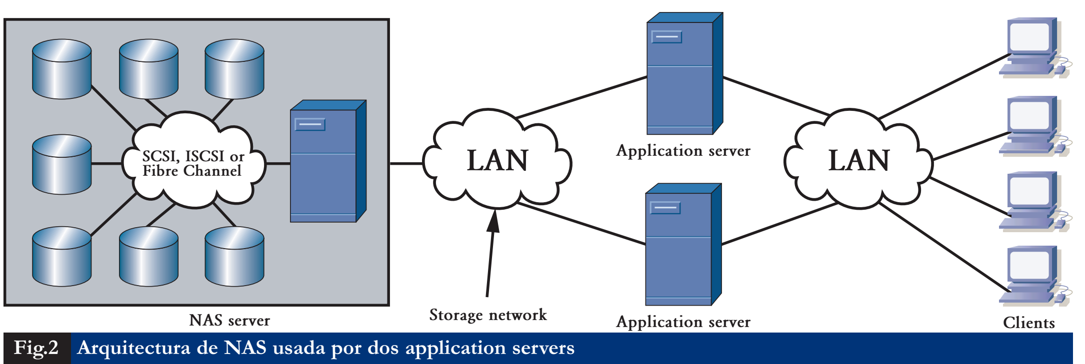


Fig.2 Arquitectura de NAS usada por dos application servers

SAN vs. NAS

De acuerdo a las limitaciones de esta tecnología, la tabla comparativa nos muestra las diferencias entre SAN y NAS, lo cual nos permite hacer un análisis de qué tecnología puede ser mas útil, de acuerdo a los requerimientos buscados en las soluciones consolidadas de storage que hay en el mercado. ●

El cambio a la tecnología de Video IP



Video Security

Lic. Gustavo C. Tonzo
Regional Sales Manager
Logicalis Latin America

En los últimos años se ha desarrollado y establecido con fuerza la tecnología de video IP orientada a la seguridad, es decir soluciones integradas de video IP y alarmas aplicadas en circuitos cerrados de TV, controles de accesos, alarmas, etc.

Desde Logicalis Latin America, como integradores con más de 20 años de trayectoria en el mercado, consideramos que la implementación de este tipo de soluciones ofrece grandes beneficios tanto en costos como en retorno de inversión, debido a la utilización de la tecnología IP.

Las soluciones de IndigoVision sobresalen en el mercado de Video IP pues no poseen un único punto de falla, permiten una ilimitada cantidad de puntos de visualización y control, sin costo adicional para el usuario así como una sencilla implementación en redes convencionales e inalámbricas.

Estas soluciones de Video IP son altamente confiables y están destinadas a la seguridad de aeropuertos, prisiones, medios de transporte, grandes eventos tales como los Juegos Olímpicos y los campeonatos mundiales, como así también lugares que requieran excelencia en la calidad de video como los bancos y casinos.

Las características principales en los que se basan las soluciones de Video IP de IndigoVision son: alta calidad de video, optimización de la utilización del ancho de banda de las redes y una importante reducción en espacio y costos del almacenamiento asociados al video. Estas características se obtienen mediante eficientes algoritmos de compresión específicamente diseñados por IndigoVision que lo posicionan a la vanguardia de las soluciones de Video IP.

De la tecnología analógica al video IP

La tecnología de Video IP implica una solución integral, con posibilidades de ampliarse y, a la vez, ofrece una mejor calidad respecto a la tecnología analógica. Por ejemplo, los costos de instalación en superficies grandes de los

FOTO: http://www.sxc.hu/ - Thomas Hansen

sistemas de video tradicionales son altísimos ya que utilizan materiales como fibra o cable coaxil. A la vez, no permiten instalar muchas estaciones de control, debido a la inversión que se necesita para duplicar un cambio costoso de infraestructura.
En general, se recomienda a las empresas hacer el cambio al video IP cuando el sistema que se está utilizando requiera mayor número de cámaras o estaciones de control o bien, cuando se desea integrar varios sistemas en diferentes lugares. En la actualidad, las empresas requieren una única solución integral que se pueda ampliar y ofrecer vigilancia por video de alta calidad en diversas oficinas o lugares, y esto es precisamente lo que proporciona el video IP.



Los módulos de transmisión/recepción IP transmiten video, audio y datos de control digitales de calidad MPEG-4 a través de la red IP.
Fuente: www.indigovision.com

Cuando se opta por una solución basada en el video IP, no hay necesidad de preocuparse de que las ampliaciones futuras del sistema vayan a superar los límites de capacidad del hardware instalado, ya que los dispositivos adicionales (cámaras, estaciones de control y grabadores de video) pueden incorporarse a cualquier punto de la red en todo momento.

Planificar el cambio

Al realizar un cambio de tecnología analógica a tecnología de video IP, es importante que el departamento de informática se vea implicado desde el principio en el proceso de planifi-



Los paneles de alarma IP permiten una fácil conexión a la red de las entradas y salidas con el fin de conectar otros sistemas de seguridad como la detección de intrusos y el control de acceso.
Fuente: www.indigovision.com

"La tecnología de Video IP de IndigoVision brinda una innovadora solución integrada de wireless CCTV para la Central Station de Amsterdam”

Cámaras IP

Una cámara IP fija o domo es una única unidad integral que contiene la propia cámara, el codec para la compresión del video y el transmisor/receptor para la red. Las cámaras domo de IndigoVision permiten un uso sencillo de los sistemas de video basados en IP, ya que sólo necesitan un único cable CAT 5 de conexión a la red.
Las cámaras IP utilizan tecnologías de compresión, que pueden ser MJPEG o MPEG-4, siendo esta última la que proporciona una calidad de video mucho mejor. Es posible usar esta tecnología en el modo de “imagen-I exclusivamente”, que es básicamente idéntico a MJPEG pero cumple con la norma MPEG-4. En dicho caso, la cámara IP puede calificarse como MPEG-4 pero tener una calidad de video similar a MJPEG.
Los domos son el punto de partida ideal para las cámaras IP más sofisticadas, ya que el tamaño físico del artefacto ofrece el espacio adecuado para alojar los sistemas electrónicos necesarios. Los costos, el rendimiento y el consumo de potencia del sensor de la cámara y del hardware de compresión MPEG-4 permiten integrarlo todo en un domo IP profesional dedicado.
El problema que presenta MJPEG es la necesidad de un gran ancho de banda para generar video de buena calidad. Generalmente se trata de entre 10 y 30 veces más de lo que necesita una buena puesta en práctica de MPEG-4. Esto tiene un gran impacto en el ancho de banda y el almacenamiento. Tanto el suministro de la red como el costo de almacenamiento tienen que ser al menos 10 veces mayores de lo que deberían ser.
De todas formas, a pesar de que las cámaras IP basadas en MJPEG generalmente son más económicas, el resto del sistema es muy costoso, lo que se traduce en un costo total del sistema mayor que el resultante en caso de utilizar una tecnología de compresión de buena calidad.



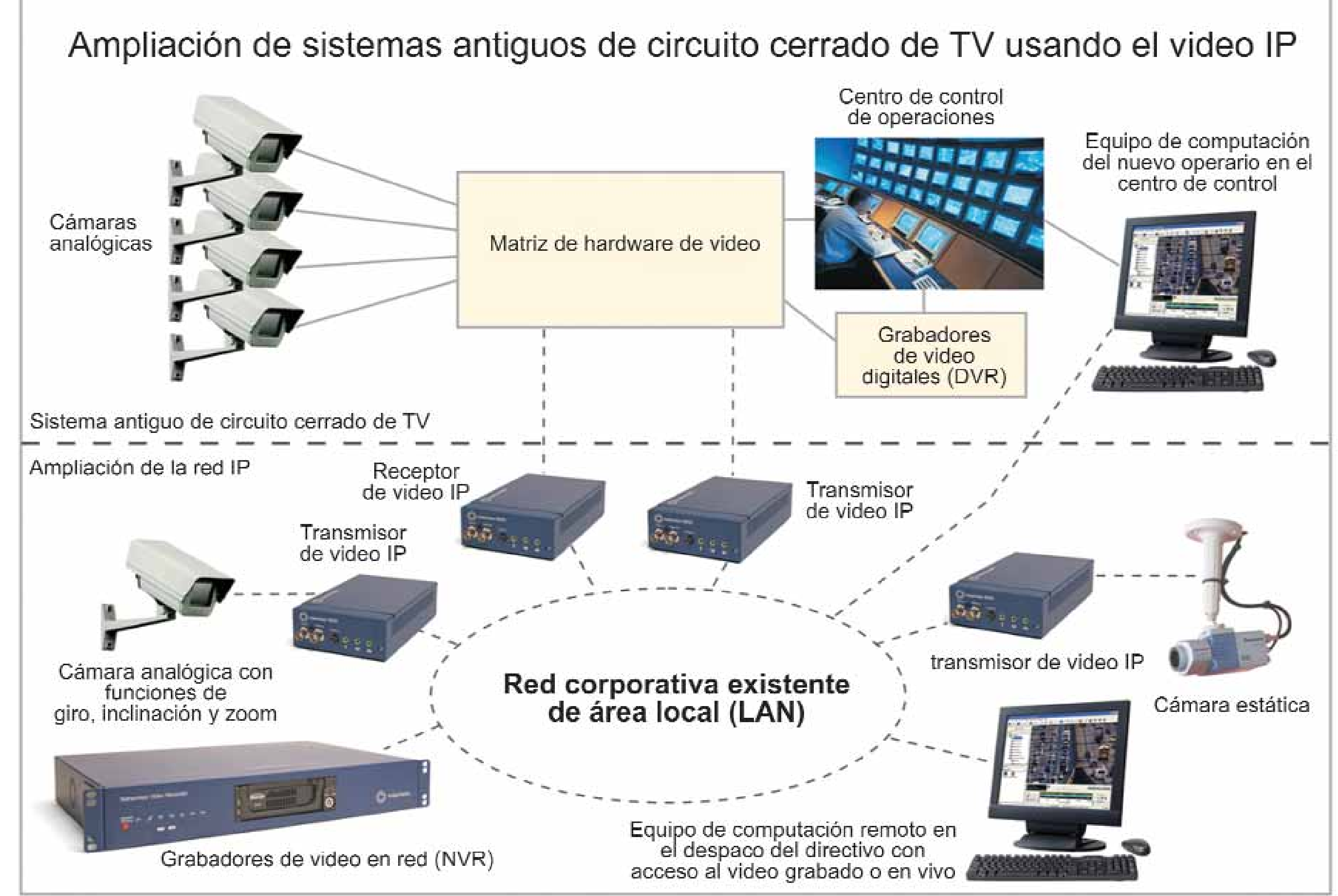

YA

cación. Los productos de video IP de IndigoVision tienen características con las que los profesionales de informática ya están familiarizados, por ejemplo el protocolo simple de gestión de red (SNMP -Simple Network Managment Protocol), los servidores de seguridad integrados, los límites de la tasa de transferencia y los programas de diagnóstico. Esto permite mantener el control del tráfico de red generado y monitorear el rendimiento del sistema y también facilitar la resolución de posibles problemas.

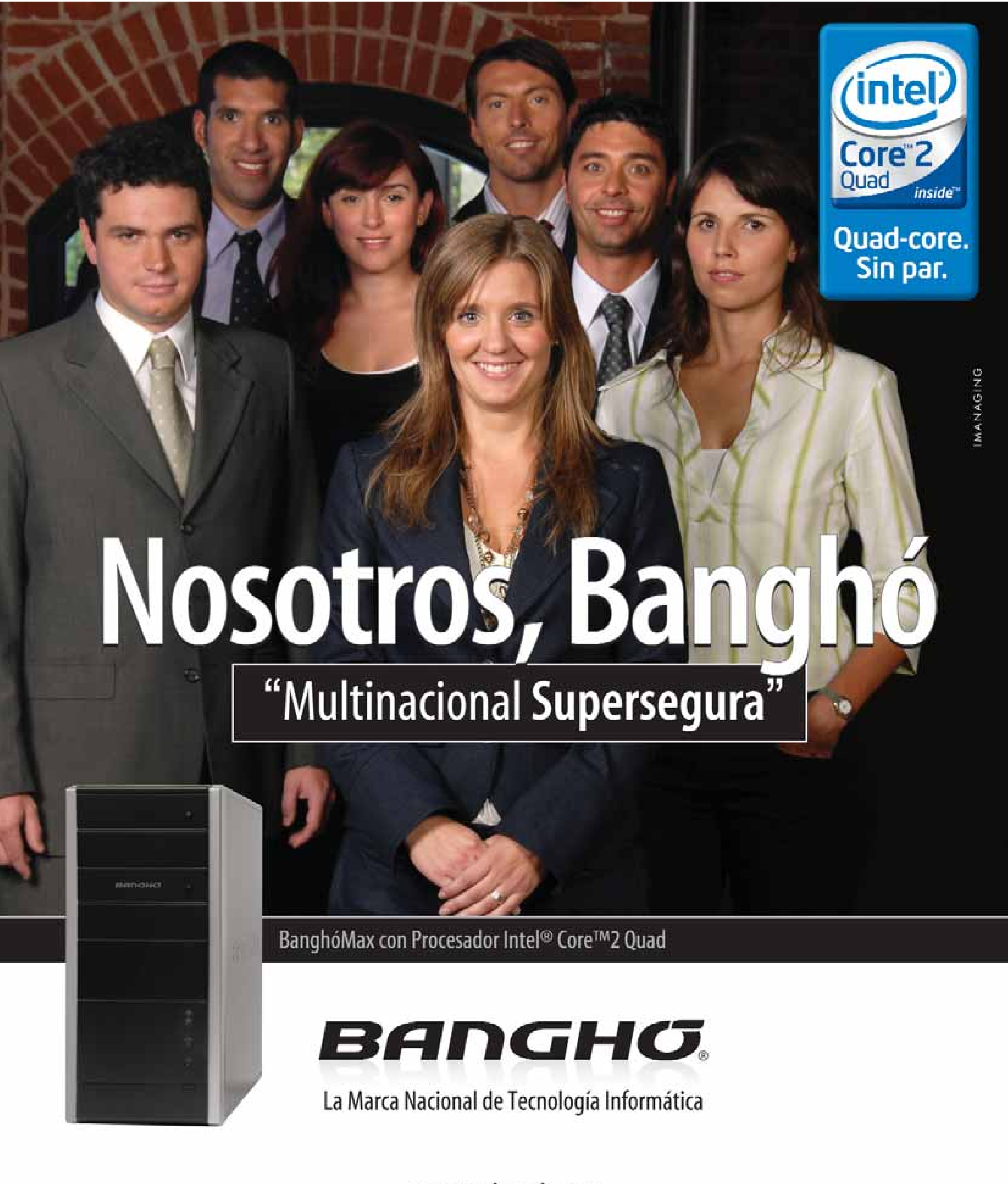
Por varios motivos se recomienda que este tipo de cambios se desarrollen en distintas fases. Principalmente esto permite comprobar que cada fase funcione correctamente antes de comenzar la siguiente. Además, existen otras ventajas: los equipos existentes pueden mantenerse y utilizarse normalmente hasta que su mantenimiento llegue a ser demasiado costoso o deje de ser práctico. El proceso de migración puede detenerse o aplazarse en cualquier momento y se puede seguir usando el sistema existente con una instalación en la que se utilice el sistema antiguo y el nuevo a la vez.

> “Las soluciones de Video IP de IndigoVision son de alta calidad de video, con optimización de la utilización del ancho de banda de las redes y una importante reducción en espacio y costos del almacenamiento asociados al video”

Por ejemplo, si es necesario ampliar un sistema existente en cantidad de cámaras y cantidad de puntos de control y no se cuenta con demasiado presupuesto, se recomienda hacer el cambio paulatinamente, con una primera fase de emplazamiento, en el que las nuevas cámaras se conectan al sistema a través de un transmisor utilizando la red LAN ya existente. Además, el uso de transmisores IP (codificadores) ofrece muchas posibilidades en la elección de las cámaras ya que cualquier cámara convencional funcionará correctamente. Los receptores IP (decodificadores) de cada cámara se conectan a una entrada de la matriz que no se esté utilizando. A su vez, las salidas de la matriz se conectarán a otros transmisores IP para llevar las imágenes de video del centro de control de operaciones a la red LAN. Las cámaras adicionales también requerirán mayor capacidad de grabado, por lo que se conectarán a la red más grabadores



Fuente: www.indigovision.com


intel
Core 2
Quad
inside
Quad-core.
Sin par.
IMANAGING
Nosotros, Banghó
"Multinacional Supersegura"
BanghóMax con Procesador Intel® Core™2 Quad
BANGHÓ®
La Marca Nacional de Tecnología Informática
www.yobangho.com

de video en red (NVR). El resto de los elementos del sistema se pueden añadir independientemente, lo que hace que la solución IP pueda ampliarse en el futuro, cuando se disponga de un presupuesto mayor.
El cambio total a un sistema IP completo se justifica por el hecho de que con el tiempo, el mantenimiento de la matriz se hace bastante problemática, además la capacidad de grabación de los grabadores DVR cada vez es menos adecuada. Es entonces que finalmente se elimina la matriz de hardware original y se convierte la red LAN y el software de control en una "matriz virtual". Para hacer que las cámaras originales sean compatibles con el sistema IP, en cada una de ellas se instalará un transmisor IP y, como éstas ya estaban unidas mediante el cableado a un punto común del centro de control de operaciones, se usarán transmisores IP montados en rejillas, que normalmente suponen un ahorro del 10 al 15 por ciento en comparación con las unidades autónomas. Los transmisores y receptores IP que estaban conectados directamente a la matriz se utilizarán de nuevo para conectar algunas de las cámaras analógicas a la red.
De este modo, transformar un sistema analógico existente en una solución IP no presenta demasiadas dificultades. Si el cambio se realiza de manera progresiva posibilita tener en cuenta las condiciones presupuestarias a la vez de analizar cada etapa de la implementación.

El sistema NVR típico solamente necesita una plataforma informática y almacenamiento en un disco duro. Se pueden presentar en unidades autónomas con discos duros extraíbles para aplicaciones más exigentes que deban soportar fallos.

Fuente: www.indigovision.com



DVR | NVR

Grabación en video digital - los grabadores NVR

Es importante distinguir entre los grabadores de video digitales (DVR) y los grabadores de video en red (NVR), ya que a menudo se denomina a ambos “digitales”.
Un DVR comprime digitalmente las señales de video analógicas y las almacena en un disco duro. El término digital se refiere en este caso a la tecnología de compresión y almacenamiento, no a las imágenes de video transmitidas. Por lo tanto, el DVR debe colocarse cerca de las señales analógicas. Por otro lado, un NVR almacena las imágenes digitales directamente desde la red IP. Por consiguiente, la diferencia más evidente entre un DVR y un NVR es que el DVR graba secuencias analógicas de cámaras analógicas, mientras que un NVR graba secuencias de video que han sido previamente codificadas por las cámaras. Así, en un NVR no existe ninguna conexión de video. Sus entradas y salidas son datos IP, que se componen de video comprimido y codificado. Los NVR pueden estar basados en software informático o ser unidades autónomas dedicadas.
La mayor ventaja de una arquitectura basada en grabadores NVR es que éstos se pueden colocar en cualquier lugar de la red: en el centro de control, cerca de grupos de cámaras, al margen de la red o agrupados en un entorno protegido. Cualquier operario puede visionar desde cualquier punto de la red las secuencias de video grabadas. Los NVR graban y muestran imágenes a la vez, y varios operarios pueden visionar simultáneamente las grabaciones de cualquier máquina desde diferentes puntos de la red de manera independiente y sin afectar a los demás operarios.
La independencia de la ubicación física es un factor fundamental. Si se calcula el tráfico de red necesario y los NVR se colocan estratégicamente en consecuencia, se puede reducir al mínimo el impacto que tiene la transmisión del video sobre el uso del ancho de banda. Normalmente el NVR se colocaría cerca de un grupo de cámaras (en términos de red, pero no necesariamente cerca desde el punto de vista físico) para que la red LAN local soporte la carga, al ser dicha red capaz de asimilarla fácilmente. Así, se ahorraría capacidad en otras partes de la red que quizás sean más limitadas. Actualmente se utilizan con frecuencia las técnicas de reflejado para hacer copias de las secuencias grabadas en NVR adicionales colocados en diferentes partes de la red. Esto proporciona un gran nivel de protección frente a un fallo de la red ya que, si se estropea una parte, siempre habrá otra de reserva.
Además, es posible tener tantos NVR a lo largo de la red como se desee, ya que no se necesita ningún cableado de video adicional.

Windows Server 2008
Servicios de Federación de Active Directory

Con el indudable crecimiento exponencial de servicios web que se han estado gestando durante estos últimos tiempos, es prácticamente inevitable la necesidad, por parte de las organizaciones, de administrar más eficientemente la forma en la que sus clientes, socios de negocios y usuarios en quienes confían acceden a sus aplicaciones. Este fenómeno, con el cual los administradores se están enfrentando día a día, los obliga a desarrollar una solución que permita gestionar las identidades y sus accesos de manera segura, proyectando el creciente número de aplicaciones con el agravante de las diferentes plataformas y tecnologías sobre las que estas potencialmente podrían llegar a correr.

Suena engorroso pensar en la administración de gran cantidad de aplicaciones web corriendo sobre diversas plataformas cuando, al mismo tiempo, se debería brindar un nivel de seguridad rigurosamente alto ya que estas aplicaciones se encuentran expuestas en Internet. Sobre todo si pensamos en satisfacer al socio de negocio o cliente con un acceso simple a nuestra red acotando la cantidad de contraseñas que los usuarios requieren para el acceso seguro, con el desafío adicional de minimizar la carga administrativa en la gestión de datos duplicados sobre los múltiples entornos, todo esto sin sacrificar el nivel alto de seguridad al cual debemos apuntar.

Ante estos desafíos, Microsoft ofrece una solución conocida como **Servicios de Federación de Active Directory** (Active Directory Federation Services), incluido en la futura versión **2008** del sistema operativo para servidores **Windows Server** y componente actual de la versión **2003 R2** del mismo sistema operativo, el cual proporciona tecnologías de inicio de sesión único (SSO) web con el objetivo de brindar a los usuarios la posibilidad de autenticarse en varias aplicaciones web durante una única sesión en línea.



Martin Sturm
Regional Project Manager
Aon Risk Services
Latin America

En la actualidad los servicios que ofrece la web han estado en constante crecimiento. Ante esta realidad Microsoft ofrece una solución conocida como Servicios de Federación de Active Directory (Active Directory Federation Services) y en esta nota les contamos de qué se trata.

En otras palabras, es una solución de identidad de accesos que brinda la posibilidad a los clientes Web, internos o externos a nuestra red, de autenticarse por única vez para el acceso a una o más aplicaciones expuestas de cara a Internet, aún cuando las cuentas de usuario y las aplicaciones se encuentren ubicadas en redes u organizaciones completamente diferentes.

Precisamente cuando una aplicación web se encuentra localizada en una red y las cuentas de

usuario utilizadas para el acceso en otra, es común que, al intentar acceder a las aplicaciones publicadas, los usuarios reciban pedidos de autenticación con cuentas secundarias. Esto se debe a que las credenciales secundarias representan la identidad de los usuarios en el reino donde la aplicación reside. El Web Server que publica la aplicación usualmente requiere de esas credenciales para poder tomar la decisión más apropiada de autorización.

Con los Servicios de Federación de Active Directory (AD FS), al proveer de relaciones de confianza utilizables para proyectar las identidades digitales y derechos de acceso de sus usuarios como socios confiables, las cuentas secundarias se convierten en innecesarias, lo que hace que en un entorno federado cada organización continúe manejando sus propias identidades pero puedan aceptar de manera segura identidades de otras organizaciones.

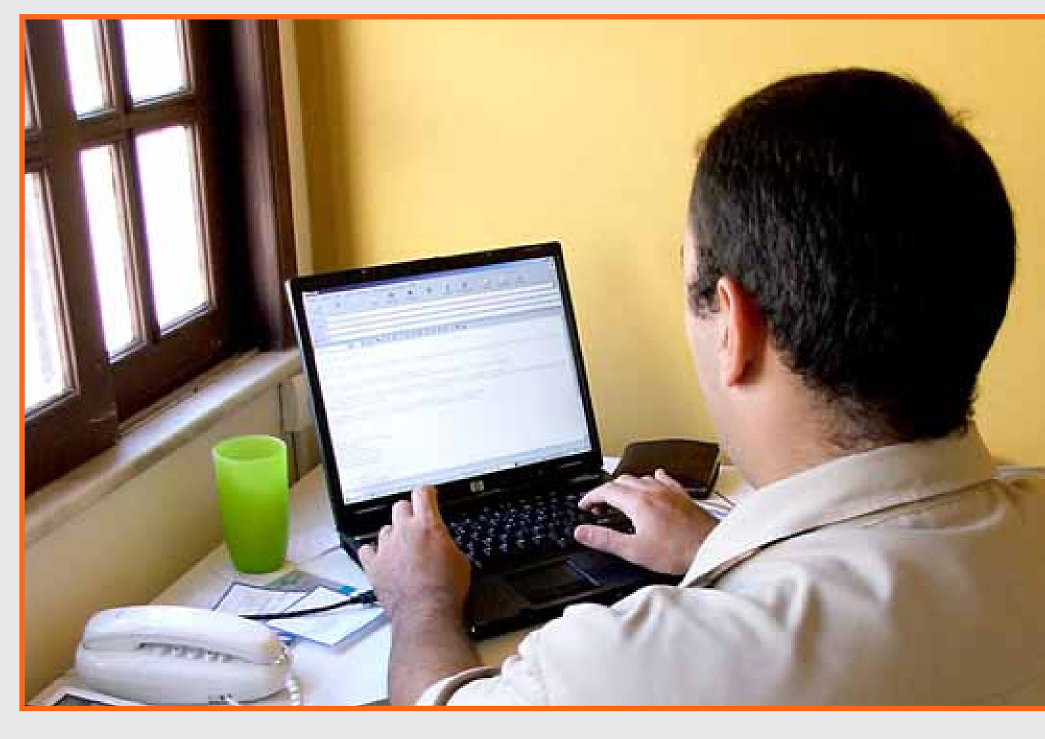


FOTO: http://www.sxc.hu/ - Bruno Neves

Actualmente existen roles bien definidos de AD FS: **Servicios de Federación** (Federation Services) que abarcan uno o más servidores y compartiendo una política común de confianza para el ruteo de peticiones de autenticación sobre cuentas de usuarios de organizaciones externas o internas quienes acceden desde cualquier punto del planeta a través de Internet. **Proxy de Servicios de Federación** (Federation Service Proxy) hacia los servidores de federación existentes en la red perimetral o DMZ mediante la utilización del protocolo **WS-Federation Passive Requestor Profile** (WS-F PRP) para la colección de la información de credenciales de usuario desde el navegador de los mismos con el objetivo de ser enviada hacia los servidores de federación en su nombre. O bien, **Servicios de Agentes Web** (Web Agent Services) utilizados para habilitar el **inicio de sesión único (SSO) web**. Al proceso de autenticación a una red y acceso a recursos de otra diferente sin la necesidad de repetición en la acción de conexión **(logon)** es conocido como **inicio de sesión único** (Single Sign-On).
Estos roles, configurados y utilizados en conjunto, permiten obtener beneficios sobre la personalización de la experiencia en el acceso y autorización de usuarios a las aplicaciones publicadas, como así también facilitar las transacciones Business-to-business (B2B), basados en dos tipos o conceptos de organización:
Organización de Recursos: Hablamos de este tipo de organizaciones cuando, aquellas que poseen y administran recursos para ser accedidos a través de Internet, implementan servidores de federación de AD FS y/o servidores Web AD FS-enabled para administrar el acceso seguro de sus socios confiables, pero que no cuentan internamente con las cuentas de usuario que serán utilizadas para dicho acceso.
Organización de Cuentas: En este tipo de organizaciones se implementan servidores de federación de AD FS para autenticar usuarios locales y crear "Security Tokens" que luego podrán ser utilizados por estos mismos dentro de una organización de recursos para tomar decisiones de autorización.

Afortunadamente, **Microsoft Windows Server 2008** incorpora una serie de nuevas funcionalidades en AD FS, no disponibles en la versión 2003 R2, diseñadas para lograr una administración aún más eficiente al, entre otras cosas, mejorar el soporte de aplicaciones disponiendo de una firme integración con Microsoft Office SharePoint Server 2007 y Active Directory Rights Management Services (AD RMS), incluir como un rol de servidor de Windows Server a AD FS, con el que se permitirá mejorar las instalaciones mediante la realización de nuevos chequeos de validación en los Wizards de instalación. Pero sin lugar a dudas, la gran mejora se ve reflejada en cómo Windows Server 2008 maneja el proceso de importación y exportación de archivos de políticas de confianza entre socios de organizaciones.

Básicamente los administradores de AD FS pueden crear una confianza federada entre dos organizaciones usando o bien un proceso de importación/exportación de archivos de políticas o usando un proceso manual que envuelve el intercambio mutuo de los valores de cada socio (partner), como lo son los indicadores uniformes de recursos (URIs), los tipos de demandas y sus mapeos, los nombres para mostrar (display names), etc.
Este proceso manual requiere que el administrador, quien recibe la información, la tipee en las páginas para agregado de socios sobre el Wizard (Add Partner Wizard), lo cual puede, claramente, resultar en errores de tipeo.

Adicionalmente el proceso manual requiere de la cuenta de administrador del socio para el envío de una copia del certificado de verificación del servidor de federación hacia el administrador del socio de recursos para que el certificado pueda ser agregado a través del wizard. Aunque este proceso de importación/exportación de archivos de políticas estaba disponible en la versión 2003 R2, la creación de confianzas federadas entre socios de organizaciones es mucho más simple en Windows Server 2008 como resultado de la mejora en la funcionalidad de import/export. Estas mejoras fueron realizadas para aumentar la eficiencia administrativa permitiendo mayor flexibilidad en la importación sobre el Wizard mis-

Notas de la Serie

#1 - Introducción

#2 - Windows Server 2008: Servicios de Federación de Active Directory

#3 - Windows Server 2008: Protección de Acceso a Red

#4 - Windows Server 2008: Server Manager

#5 - Windows PowerShell

#6 - Mejoras en la pila Next Generation TCP/IP

#7 - BitLocker Drive Encryption

mo. Por ejemplo, cuando una política de socio es importada, el administrador puede usar el Add Partner Wizard para modificar cualquier valor importado antes que el proceso del Wizard sea completado. Esto incluye la habilidad de especificar un certificado de verificación de cuenta de socio diferente y la habilidad de mapear las demandas entrantes y salientes entre los socios.

Usando la funcionalidad de export e import incluidas con AD FS in Windows Server 2008, los administradores podrán exportar de manera muy simple sus configuraciones de políticas de confianza a un archivo .xml y luego enviarlo al administrador socio. Ese intercambio provee todos los URIs, los tipos de demandas, los nombres para mostrar y otros valores junto a los certificados de verificación que son necesarios para crear confianzas federadas entre dos organizaciones socias.

En definitiva, si bien dispondremos de notables mejoras y nuevas funcionalidades en los Servicios de Federación de Active Directory sobre Windows Server 2008, la versión ya existente sobre 2003 R2 nos permitirá implementar, hoy en día, una solución de federación entre entidades externas lo suficientemente robusta, segura y confiable que pueda ajustarse perfectamente a las necesidades y requerimientos corporativos. ●

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)®

Un certificado seguro

Conozca cómo es el proceso para obtener la certificación CISSP y cuáles son sus beneficios y problemas. NEX IT habló con Ezequiel Sallis, experto en seguridad de la información quien nos dio algunos consejos para tener en cuenta.

Las certificaciones dentro del mundo IT son muy importantes por su reconocimiento y por las posibilidades laborales que brindan. Cada vendor tiene sus propias certificaciones, las cuales generalmente están relacionadas con algún producto o aplicación en particular y certifica que el profesional las conoce en profundidad. Sin embargo existe una que no está ligada a ningún vendor y aún así es reconocida mundialmente y es el referente en lo que hace a la seguridad de la información. Hablamos de la certificación CISSP (Certified Information Systems Security Professional).

CISSP es otorgada por la (ISC)² (International Information Systems Security Certification Consortium, Inc), con el fin de certificar y reconocer a aquellos profesionales con formación en el área de la seguridad.

NEX IT habló con Ezequiel Sallis, Senior Security Specialist y uno de los 46 CISSP que existen en nuestro país, quien nos comentó un poco más acerca de esta certificación, sus mitos y beneficios.

Examen

Para obtener la certificación CISSP se debe rendir un examen presencial que consta de 250 preguntas del tipo multiple choice con cuatro opciones de las cuales solo una es la correcta. "Lo bueno de este examen es que no existen trampas ni preguntas ambiguas pero puede ser que en una pregunta todas las opciones sean correctas y en ese caso se debe elegir de las correctas, la mejor", comenta Sallis.

La certificación consta de 10 dominios de conocimiento que conforman el Common Body of Knowledge (CBK). Estos dominios están orientados al Control de Acceso, Seguridad en Telecomunicaciones y Networking (redes), Administración de Seguridad, Seguridad en Aplicaciones y Sistemas, Criptografía, Modelos de Seguridad y Arquitectura, Seguridad Operativa, Business Continuity Planning y Leyes, Investigación y Ética.

"Examen exigente pero justo"

En las 250 preguntas se abarca por completo el CBK, pero no existe la misma proporción de preguntas por dominio ya que las preguntas seleccionadas para esa instancia son random. Además, existen 25 preguntas no identificadas que son a modo de prueba y que su respuesta no cuenta a la



CentralTECH
Capacitación Premiere
Aula Laboratorio CentralTECH
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
(CISSP)
El Mejor Centro Training Security 2007 para Sudamérica Sur
La Certificación CISSP está diseñada para reconocer y garantizar su experiencia en Seguridad Informática. Enriquece su carrera profesional, brindando mayor credibilidad y una Muy Importante Salidad Laboral.
Si Estás Certificado, estás Tranquilo.
CISSP Wireless Security - $ 4189 + IVA
CISSP Esp. Microsoft - $ 5278 + IVA
CISSP Esp. Linux - $ 4718 + IVA
CentralTECH Capacitación Premiere | +54 (11) 5031.2233-34
masinfo@centraltech.com.ar | www.centraltech.com.ar/security.asp
Av. Corrientes 531 - Primer Piso - Capital Federal

hora de la calificación. "Es un testeo para saber si las preguntas se entienden, si su enunciado está bien redactado y de esta forma se mejora y se renueva el cuestionario", explica Sallis.

El examen es presencial y, a diferencia de la mayoría de las certificaciones, es escrito y sin computadoras de por medio. Originalmente el examen era en inglés, luego se incorporó el chino, y finalmente el italiano, el español, etc. Actualmente se puede elegir el idioma en el que se quiere rendir, pero igualmente es bilingüe. Es decir que si se elige en español también figuran las preguntas en inglés para evitar los problemas de traducción. Lo que sí se permite es tener un diccionario palabra-palabra, sin definiciones, para quienes que deciden rendir en un idioma no nativo.

El examen se aprueba con 700 puntos pero no todas las preguntas tienen el mismo valor. "Es por esto que no es posible hacer cálculos de cuántas debo responder correctamente para aprobar ya que además dentro del total se incluyen las 25 de pruebas que no se saben cuáles son", enfatiza Ezequiel Sallis.

A los 10 días hábiles de haber rendido el examen aproximadamente se recibe la nota por mail; el proceso siguiente es el de la certificación propiamente dicha. Para obtenerla un CISSP debe firmar un endorsement y adjuntarle el currículum u hoja de vida y enviar toda la información al (ISC)². El proceso de certificación tiene una duración de tres años y luego de ese período, y cada tres años nuevamente, se deben juntar 120 puntos de educación continua (CPE - Continue Professional Education) para revalidar la certificación. Los *puntos A* tienen relación con todo aquello que realice el profesional en relación a los 10 dominios de la certificación. Los *puntos B* son las actividades que lo hagan crecer como profesional, como por ejemplo ejercitar un idioma no nativo, cursos de management o de marketing, leer un determinado libro, cursar o dictar un curso, escribir un artículo, etc. Toda esta información se debe cargar en la página web del (ISC)² mediante un usuario y contraseña.

> "Para el (ISC)² **no** existe **diferencia** entre los **CISSP**, es por esto que al aprobar el examen no te dan una **nota**"

Requisitos

Toda persona que quiera convertirse en un CISSP debe cumplir con algunos requisitos.

El principal es aprobar el examen. "Es exigente pero justo, por lo que si se está adecuadamente preparado no es imposible de aprobar", afirma Sallis. Para esto se debe tener un puntaje de 700. Además se deben tener cinco años de experiencia en por lo menos dos de los 10 dominios sin importar la proporción. O bien, cuatro años de experiencia y un título de grado sin importar la orientación. A partir del 1 de octubre de 2007 la cantidad de años de experiencia aumentará a cinco, pero no afectará a quienes rindan esta certificación antes del 30 de septiembre. Sin embargo, se puede primero rendir el examen, luego alcanzar los años de experiencia y una vez allí tramitar la certificación. Pero este proceso no es lo recomendable.

Finalmente los aspirantes deben adherirse al Código de Ética de la (ISC)².

Perfil

"Muy pocas personas entienden lo que implica convertirse en un CISSP", afirma Sallis. Esto es porque el conocimiento que brinda la certificación es muy amplio y abarca desde los aspectos técnicos hasta los legales y de management. Ezequiel Sallis, uno de los pocos con esta certificación, comenzó a los 19 años con la parte técnica y, aunque actualmente es especialista de la seguridad de la información, está terminando la carrera de abogacía. "Si te sorprendes de esto es porque no comprendés de qué se trata ser un CISSP", sentencia.

Los aspirantes a esta certificación vendor independent apuntan a convertirse en Oficiales de la Seguridad dentro de una organización. El problema principal en las organizaciones es que es muy difícil la comunicación entre los profesionales muy técnicos y los de management, "la certificación es un lenguaje en común", agrega.

Problemáticas

Uno de los problemas que surgen a la hora de prepararse para rendir el examen es la gran variedad de bibliografía. Existen muchos libros y mucha información pero sin un camino o una guía clara se corre el riesgo de terminar sabiendo mucho de nada.

La continua actualización es un requisito indispensable para cualquier profesional de la seguridad. Nuevas vulnerabilidades y amenazas nacen minuto a minuto y el no estar al tanto de ellas hace que nuestro sistema pueda sufrir algún ataque. "Quizás el irse de vacaciones hace que uno pierda información que puede ser clave", sentencia Sallis.

El último problema que existe es que las empresas buscan solamente a un solo profesional de la seguridad y esperan que pueda solucionar todos lo problemas sin darse cuenta que en estos casos el trabajo en equipo es lo más efectivo. Además la certificación CISSP da los conocimientos técnicos y gerenciales pero igualmente se necesita un team al cual poder dirigir y con el cual poder trabajar.

Beneficios

Hoy en día lograr la seguridad es una de las principales problemáticas en la mayoría de las empresas. El filtro y robo de información, las vulnerabilidades crecientes y la ingeniería social son los puntos a combatir. Pero para lograrlo se necesita alguien capacitado y con los conocimientos adecuados.

En nuestro mercado el tener la certificación CISSP es una variable competitiva muy importante, ya que la cantidad de certificados que existen en nuestro país hoy por hoy sigue siendo reducida. En Argentina existen solo 46 profesionales con la certificación CISSP y a nivel mundial 48.598. La poca oferta y la gran demanda hacen que cualquiera que sea un CISSP pueda obtener muy buenas ofertas laborales y, lógicamente, una excelente remuneración.

"Si bien el camino es largo, el premio y la satisfacción al final bien lo valen", concluye Sallis.●

Consejos

Si un profesional decide afrontar la experiencia de prepararse para rendir la certificación CISSP, lo más conveniente es asistir a cursos preparatorios en donde se puede formar un equipo de estudio y aprender de las dudas e inquietudes de los demás. De todas formas, es algo que depende de la disciplina de la persona. Lo recomendable es tener un cronograma de estudio y 2 ó 3 meses de preparación intensa previa.

¿Exámenes tipo? Los más cercanos al examen real son los que se pueden descargar de la página www.cccure.org. Son exámenes abiertos y gratuitos del cual se obtiene un porcentaje de eficiencia, cuánto se tardó por pregunta y al loggearse con el mismo usuario trata de no repetir las preguntas.

Libros Recomendados

- **CISSP All-in-One Exam Guide** de Shon Harris
- **Official (ISC) Guide to the CISSP Exam**
- **Information Security Management Handbook**
- **Computer Security Basics** de Deborah Russell
- **Practical Unix & Internet Security** de Simson Garfinkel
- **Applied Cryptography: Protocols, Algorithms, and Source Code in C** de Bruce Schneier
- **Information Security Policies Made Easy** de Charles C. Wood

Acceso remoto para la asistencia técnica

Sebastián Passarini
Administrador de Redes

Serie "IT PRO en PyMEs II" Nota #3

Asistir a nuestros usuarios en forma personal es una buena práctica, aunque requiere de tiempo para el traslado. Hoy en día con el uso de herramientas de acceso remoto, podemos hacer prácticamente lo mismo reduciendo los costos de soporte.

Son las 09:00 A.M. de un día lunes y un usuario nos llama indicando que tiene problemas con una fórmula de Excel. Cuando nos dirigimos hasta el puesto de trabajo descubrimos que es un error de sintaxis, ya que el usuario no estaba seguro de cómo utilizar una función determinada. Volvemos a nuestro puesto de trabajo luego de 20 minutos aproximadamente cuando recibimos otro llamado de un usuario que no recuerda cómo cambiar su password en el sistema transaccional de la compañía y, la verdad, que como el mismo está un tanto desactualizado y no se integra con Active Directory, debe hacerlo manualmente. Nuevamente, dado que es muy complicado guiarlo vía telefónica, debemos movernos hasta su puesto de trabajo. Al regresar, luego de otros 20 minutos, nos preguntamos, ¿no hay otra forma más sencilla de resolver estos problemas? Entonces vienen a la memoria esas aplicaciones de acceso remoto que un colega comentó en alguna reunión. ¿Cómo se llamaban? ¿VNC, RDP, Remote Assistance?

Lo cierto es que, actualmente, contamos con varios métodos de acceso remoto y varias aplicaciones para realizar esto. El punto es: ¿todas sirven para lo mismo? ¿Da lo mismo utilizar una u otra? Creo que la respuesta es: "¡Claro que No!". Y es por esto que a continuación pasaremos a detallar y a descubrir para qué sirven cada una de estas herramientas, como así también cuándo conviene usar una u otra.

VNC Server

Esta debe ser sin duda, tal vez por ser gratuita y por su buen funcionamiento, la herramienta más difundida e implementada de acceso remoto. Con ella podemos establecer una conexión a un equipo Servidor de VNC mediante un cliente llamado VNC Viewer. Puede correr como un servicio del sistema sin importar la plataforma, Windows o Linux, ya que ambos sistemas operativos soportan la instalación del producto. Lo que obtenemos del lado del cliente es una terminal visual, que muestra exactamente lo que está ocurriendo en el equipo al que nos conectamos, y que actúa como VNC Server. Una vez establecida la comunicación con un servidor VNC, el control del mouse y teclado se comparte con los de nuestra estación, así como también la pantalla, permitiendo hacer uso de los mismos como si estuviésemos sentados frente al equipo. VNC, Real VNC, TightVNC, etc., hacen básicamente lo mismo y permiten configurar una password de acceso, es decir que si no tenemos dicha password no podremos acceder al servicio. La versión de nuestro interés se llama UltraVNC, la que podemos descargar desde los links de referencia y que cuenta con algunas opciones interesantes, como ser: File Transfer, Chat, Display Query Window y Disable Local Inputs, entre otras. De estas creo que se destaca la opción "Display Query Window", la cual permite la conexión remota de un técnico de soporte, solo si el usuario logueado en el equipo servidor acepta dicha conexión. Cuidado con esta opción, y solo habilítenla en equipos que tengan un usuario del otro lado, por ejemplo, en las PCs de nuestros clientes internos. Esto, como veremos más adelante, nos ayudará a evitar problemas del tipo confianza-privacidad. Traten de no activar esto en servidores remotos Windows NT, por ejemplo, a los que nadie tiene acceso.

"El Remote Desktop Protocol es muy utilizado por los administradores Microsoft ya que podemos administrar nuestros servidores en forma remota y conectar en una sesión establecida con un equipo remoto nuestros recursos locales"



Fig. 2

UltraVNC Repeater

Es una función más que interesante: es un add-on que podemos utilizar para conectarnos a cualquier servidor VNC de nuestra intranet, utilizando como nexo una PC puente (nuestro VNC Repeater). ¿Y para qué queremos una PC puente si podemos conectarnos directamente? Esto es válido cuando tenemos acceso a las PCs dentro de una misma intranet. Ahora bien, imaginemos que deseamos conectarnos a una PC de nuestra empresa pero desde Internet, es decir, nosotros estamos en una conferencia, curso, hotel y nos llaman solicitando el soporte remoto. En este caso, y con esta tecnología, deberíamos conectarnos a nuestra PC puente, la que luego se encargará de direccionarnos con el server VNC deseado. Para lograr esto debemos configurar en nuestro Firewall una regla de port forwarding, es decir que cuando nuestro firewall recibe una conexión al puerto 5900 (este es el puerto en que trabaja VNC), la misma sea redireccionada a nuestro VNC Repeater. De esta forma solo debemos configurar un único acceso en lugar de crear reglas para cada uno de nuestros servidores VNC internos. Recomendación: habiliten este servicio solo cuando lo vayan a utilizar, no queremos que personas ajenas a nuestra empresa logren acceso a la misma.

Fig. 1

¿Nos están espiando?

En más de una oportunidad he recibido comentarios de usuarios, los que una vez enterados de la existencia de esta herramienta comienzan a sospechar que, así como la utilizamos para dar soporte remoto, también podríamos utilizarla para espiar sus acciones y/o uso que le dan a las PCs. Este es un tema delicado, y al que no debemos darle la espalda, ya que una persona que se siente espiada/perseguida de seguro no rendirá como aquella que trabaja tranquila. Y bien podríamos decir "quien no hace cosas raras, no debería preocuparse", pero lo cierto es que son muchos los usuarios y muchas las personalidades, por lo que conviene tener un speech preparado ante la aparición de estas consultas. En mi caso, siempre les explico que se trata más que nada de una relación de confianza, y que siempre serán informados al momento de realizar una conexión contra sus PCs. Por otro lado, el cliente VNC dispone de un icono de estado, el que cambia de color cada vez que alguien se conecta. Esto los deja un poco más tranquilos, aunque como administradores lo podemos ocultar. La última versión del Cliente/Servidor Ultra-VNC posee una opción de confirmación de conexión (ver figura 1) la cual elimina este problema, por supuesto siempre que la misma esté configurada en el servidor, cosa que como Administradores deberíamos setear en las PCs de los usuarios.

Nuevamente, es un tema delicado y debe ser implementado con mucho cuidado para que el personal de nuestra empresa no se sienta incómodo.

Uso recomendado: en sistemas operativos como Windows XP/Vista tenemos otras herramientas que veremos más adelante, pero en versiones como Windows 2000 y/o Windows NT no tenemos muchas opciones por lo que es totalmente recomendable el uso de esta herramienta.

Remote Desktop Protocol o RDP

Dejando atrás los problemas de confianza y privacidad, llega a nuestro set de herramientas el cliente RDP. Cliente que viene pre-instalado en los sistemas operativos Windows XP, Windows Server 2k y superiores. Luego, para sistemas operativos como Windows 9x, Windows Me, Windows NT 4.0 o Windows 2000 será necesario bajar dicho cliente desde la web de Microsoft. La conexión cliente-servi-

Acerca de Sebastián Passarini



Sebastián Passarini es Administrador de Infraestructura y Seguridad Informática en Válvulas Precision de Argentina. Durante sus 10 años de experiencia en el área informática ha tenido la oportunidad de trabajar en Hewlett Packard Arg, entre otras empresas. Ha realizado varios cursos de tecnología y ha obtenido la certificación MCP de Microsoft. Actualmente es estudiante de la carrera de Sistemas y espera graduarse el próximo año.



NETWORK

© 2005 Juniper Networks

"Muchachos, preparen sus pistolas sedantes, nuestra red se volvió loca porque no puede seguirle el ritmo a nuestros usuarios, Oh... ¿Por qué no llamamos a Juniper desde el principio?"

>> **¿La seguridad no da abasto?** ¿Están agregando sucursal tras sucursal, usuarios remotos y dispositivos tras dispositivos en su red? Entonces llame a Juniper Networks para tener acceso remoto garantizado y seguro. Nuestras soluciones VPN, flexibles, líderes en la industria, aseguran su red vigorosamente, y a la vez entregan un desempeño extraordinario, para una excelente experiencia hacia el usuario. Visite **www.juniper.net/vpnguide** para información sobre cómo seleccionar la mejor solución VPN para su empresa. Tener un servicio confiable y desempeño asombrosamente superior es fácil: Coloque Juniper en su Red!



+54 11 4590.2453

dor se realiza a través del puerto TCP 3389 y la validación puede realizarse tanto con cuentas de AD como con cuentas locales del servidor. Esta tecnología es la más utilizada por los administradores Microsoft ya que con ella además de administrar nuestros servidores en forma remota, práctica muy recomendada por Microsoft, podemos conectar en una sesión establecida con un equipo remoto nuestros recursos locales, como ser unidades de disco e impresoras. Con esto podemos transferir archivos entre el cliente y el servidor en forma transparente e incluso imprimir en nuestras impresoras locales (las impresoras del cliente). Cuando realizamos una conexión utilizando nuestro cliente RDP en el servidor pueden ocurrir varias cosas. Si la conexión la realizamos contra un equipo Windows XP remoto, el proceso bloqueará la estación remota y nos permitirá ingresar con las credenciales correspondientes. En caso de que al momento de realizar la conexión estuviese trabajando algún otro usuario, el mismo será deslogueado automáticamente, nos logueará a nosotros y a continuación bloqueará la estación de trabajo. Una vez desconectados de la sesión, los usuarios del equipo podrán acceder normalmente ingresando sus credenciales. Luego, si realizamos la conexión contra un servidor Windows 2003, podremos tener al mismo tiempo 3 sesiones corriendo sobre el mismo sistema operativo, dos Terminal Server o Clientes RDP y una local. Por último podemos adquirir licencias de Terminal Server para aumentar la cantidad de sesiones disponibles, aunque esto ya es un capítulo aparte. En la figura 2 podemos ver una pantalla de inicio de sesión RDP con sus opciones.

Uso recomendado: administración remota de servidores Windows 2k y superiores. Implementación de Thin-Clients. La pantalla no se comparte, motivo por el que los usuarios remotos no verán las acciones que realizamos sobre el equipo.

Remote Assistanse

La Asistencia Remota trabaja casi de la misma manera que RDP, con la diferencia que en este caso tanto el usuario final como el técnico de soporte pueden realizar las solicitudes de conexión. Ambos participantes ven al mismo tiempo la pantalla del servidor, es decir, la pantalla de la PC del usuario que necesita ayuda. La conexión se establece bajo el consentimiento del usuario remoto, por lo que ya no debemos preocuparnos de los problemas de privacidad mencionados anteriormente. Es más, el primer acceso al escritorio remoto se realiza en modo visual o modo "solo ver pantalla", debiendo pedir autorización al usuario logueado en la estación remota para tomar el control de la misma. Es una herramienta muy utilizada para los casos en los que debemos resolver problemas y en los que necesitamos que el usuario, por una cuestión de capacitación, pueda ver de qué manera respondemos a su consulta. Por ejemplo, podemos realizar formulas de prueba en un Excel o explicarle cómo utilizar el formato condicional. Las aplicaciones para esta solución son muchas y no se limita a usuarios de una red empresarial o con un dominio de AD, sino que la asistencia remota también se puede brindar a PCs personales de amigos y/o familiares que necesiten de nuestra ayuda. Una persona puede solicitar asistencia remota tanto desde las opciones de "Centro de ayuda y soporte técnico de Windows XP" en un entorno de red corporativo, como así también desde la opción "Solicitar Asistencia Remota" provista con el Windows Messenger o MSN, acción que permitirá a alguno de nuestros contactos conectarse a nuestra PC para darnos soporte.

Otras opciones para solicitar asistencia remota podrían ser mediante el uso de un archivo guardado o desde el correo electrónico. Y aunque la opción más común es mediante el MSN o mediante la Ayuda y soporte de Windows XP, para entornos hogareños y empresariales respectivamente, pueden encontrar toda la documentación necesaria en la página web de Microsoft mediante los links de referencia brindados en este mismo artículo. En la figura 3 podemos ver cuáles serían los pasos para que un usuario solicite asistencia remota y en la figura 4 vemos las acciones disponibles cuando establecemos una conexión de este tipo.

Uso recomendado: asistencia remota a usuarios corporativos y/o hogareños. Altamente recomendado para brindar a un usuario soluciones que luego él mismo podrá aplicar (capacitación). En este caso es el mismo usuario quien nos dará el "OK" para acceder a su equipo y para poder tomar control del mismo.

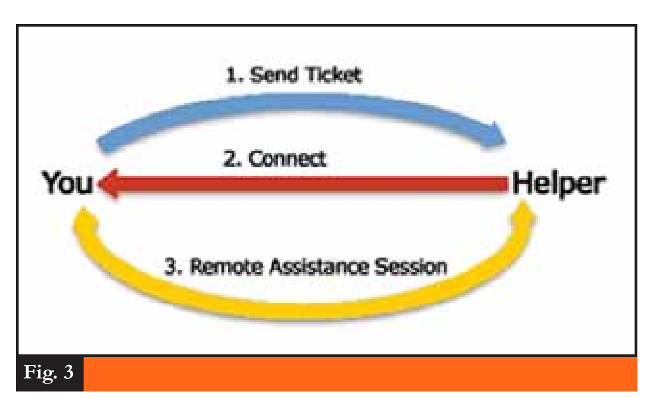


Fig. 3

"La opción Display Query Window permite la Conexión Remota de un técnico de soporte"

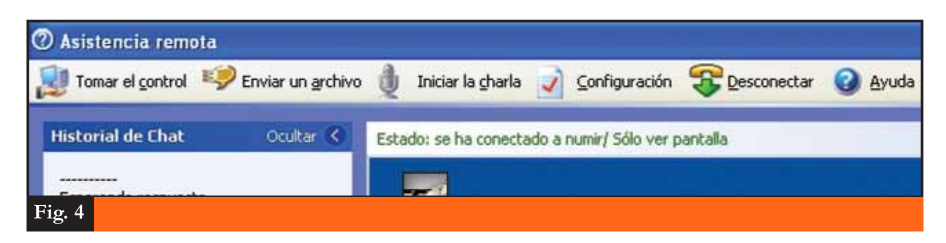


Fig. 4

Advertencia de Seguridad

Si bien hablamos de port forwarding, lo cual es una opción válida para acceder desde Internet, traten siempre de realizar implementaciones utilizando clientes VPN. Esto nos dará un mayor control sobre quién accede a nuestra red, como así también sobre los permisos que tiene en la misma.

Conclusión

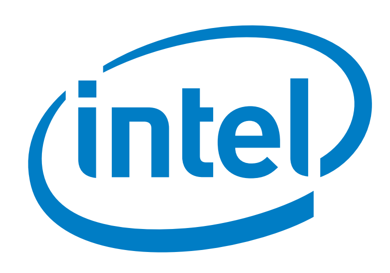
Herramientas de acceso remoto hay muchas, con costo y sin costo como las mencionadas en este artículo. Nosotros debemos, una vez analizadas las opciones, decidirnos por la que más nos convenza y convenga. ●

Libros de Referencia

http://www.uvnc.com/index.html

http://www.microsoft.com/latam/windowsxp/pro/usando/tutoriales/remotedesktop/default.asp

http://www.microsoft.com/latam/windowsxp/pro/biblioteca/deployment/remoteguide/default.asp



Time is Money

Tecnología Intel de gestión activa que permite ahorrar tiempo y dinero a los administradores IT.

Ing. Marisabel Rodríguez
Networking Supervisor

Administración Remota de Laptops con Motherboards Intel - Tecnología Intel de gestión activa.

Hablamos con Ariel Cymberknoh de Intel en Jerusalem sobre un lanzamiento del mes de mayo de este año. Este nuevo producto no es un procesador sino una plataforma, o sea un paquete completo de componentes que incluyen el procesador central además de chips secundarios que agregan capacidades tales como conectarse a una red inalámbrica. El corazón de esta plataforma es la combinación de procesador, chipset y placa de red inalámbrica, que apodaron en Intel como "Santa Rosa". Las notebooks basadas en esta plataforma se comercializarán como Centrino Pro. Intel hizo un upgrade de estos tres elementos, en su esfuerzo por incrementar la performance de las notebooks reduciendo el consumo.

Marisabel Rodríguez: ¿Cuál es la novedad de este lanzamiento de Intel?

Ariel Cymberknoh: Una característica importante del chipset es el soporte para AMT (Active Management Technology), que fue parte de la plataforma Intel vPro por un tiempo, pero se mejoró para Santa Rosa. Este tipo de administración fuera de banda (out-of-band) es en realidad una computadora completa y separada con su propia conexión a la red, con la posibilidad de operar inclusive cuando el procesador principal no está funcionando. La versión Santa Rosa de AMT 2.5, puede permitir la conexión inalámbrica. Para calificar como usuario de Centrino Pro, el sistema debe incluir el firmware AMT 2.5 y AMT/VT-BIOS, además de los demás elementos de Santa Rosa. En las notebooks para usuarios no corporativos, que no necesiten estas capacidades, la marca es Centrino Duo.

AMT en particular está orientado a los departamentos de IT de grandes corporaciones. Este grupo de personas se encarga de brindar servicios de informática y conectividad a los empleados de una empresa. Una de las tareas principales que tienen es dar soporte ante fallas de software y hardware. Cuando el número de personas que tienen que atender es muy grande, es imprescindible que atiendan los llamados y solucionen los problemas conectándose en forma remota a los puestos de trabajo. Si los equipos cuentan con esta nueva tecnología, los técnicos de IT podrán resolver situaciones en forma remota, y no tendrán que acercarse al puesto de trabajo del empleado para arreglarle la máquina porque pueden tener una visión a nivel BIOS del equipo desde su oficina. Ahora inclusive si son usuarios móviles.

Pero en definitiva los verdaderos clientes de Intel son los fabricantes de equipos que compran motherboards y arman productos OEM. Específicamente los productores de laptops, ya que este modelo nuevo en particular agrega ca-

Plataforma Santa Rosa

Es el nombre en código que se refiere a la cuarta generación de la plataforma Centrino. La Plataforma Santa Rosa fue presentada oficialmente el 9 de mayo de 2007, siendo sus principales características un CPU Core 2 Duo (Merom de 2ª Generación); un Chipset Mobile Intel® 965 Express (con gráficas integradas X3000), e Intel® Next-Gen Wireless-N Network Connection.

Esta nueva generación se comercializa con los nombres de Centrino Duo y Centrino Pro.

FOTO: http://www.sxc.hu/ - Oliver Isailovic



racterísticas orientadas a los usuarios móviles, como por ejemplo la posibilidad de conectarse remotamente vía wireless, indicación de carga de batería, entre otras posibilidades.

La tecnología está basada en firmware; permite que el equipo se comunique de manera inalámbrica a través de drivers especiales que no precisan que el sistema operativo esté levantado. Esta solución viene integrada dentro del mismo motherboard donde está la placa de red. Está específicamente diseñada para PCs de usuarios móviles y no para servidores. Para una empresa con pocos empleados este avance no significa mucho, pero cuando estamos hablando de miles de usuarios, la diferencia de costo es muy importante.

"La tecnología AMT está basada en firmware y permite que el equipo se comunique de manera inalámbrica con drivers especiales que no precisan que el sistema operativo esté levantado"

MR: ¿Qué es AMT (Advanced Management Technology)?

AC: AMT es una tecnología propietaria de Intel diseñada para dar mayores prestaciones al departamento de IT de empresas con una cierta cantidad de usuarios de PC. Permite hacer diagnósticos de problemas remotamente, mandar alarmas por aumento de temperatura en el motherboard o apertura de chasis. Para ello necesita una consola central, en donde se reciben los mensajes en tiempo real. Por ejemplo ante una alarma de temperatura, el administrador puede apagar un equipo en forma remota, o sino también luego encenderlo en forma remota, siempre independizándose del sistema operativo.

Esta tecnología está incluida en algunos chipsets especiales, y en general se estaba distribuyendo para equipos de la línea Enterprise, no para el hogar. Las empresas que fabrican equipos OEM tendrían que pagar un adicional para tener AMT en los motherboards que utilicen.

AMT ya fue probada satisfactoriamente en desktops y servidores, pero este es el primer motherboard que viene especialmente diseñado para equipos móviles. La tendencia en el mercado indica que las empresas se están volcando cada vez más a comprar laptops para sus empleados, por ejemplo hay empresas que poseen decenas de miles, y si gran parte de ellos utiliza equipos móviles, sería muy difícil realizar una administración centralizada.

MR: ¿Qué beneficios adicionales trae para los administradores de redes?

AC: Hay muchas herramientas de distribución gratuita que sirven para conectarse por red a las PCs de los usuarios y resolver proble-

mas, por ejemplo VNC, PC Anywhere o el protocolo de Remote Desktop de Windows. Gran parte de las situaciones que resuelve el departamento de IT se solucionan con estas herramientas. Pero el problema de esos sistemas es que dependen de que la máquina esté funcionando y que esté conectada a la red. Por ejemplo si el sistema operativo tiene una pantalla azul (porque se colgó), o el disco está corrupto, ningún programa funciona y el técnico tiene que acercarse al lugar donde se encuentra la PC o sino el usuario tiene que dejar su puesto de trabajo para llevársela al especialista. Esto puede ser muy sencillo cuando la empresa es pequeña, pero conlleva costos operativos muy grandes cuando hay miles de puestos de trabajo que atender o para usuarios o servidores que se encuentran en sucursales remotas donde no hay soporte de IT.

AMT crea un subsistema paralelo e independiente del CPU central de la máquina que corre sin importar qué pasa con el Sistema Operativo. Permite que el sistema esté conectado constantemente a la red y de esta manera esté disponible para solucionar problemas. Para lograr esto necesita otro procesador mucho más sencillo que el principal, y drivers de la placa de red que se cargan sin presencia del Sistema Operativo.

También se agrega una característica importante para los administradores de la red corporativa que es "Agents Presence". Dado que los propietarios de las empresas son los dueños de la información que manejan los empleados, y son responsables ante la ley por las consecuencias de las acciones de ellos (según la ley federal de Estados Unidos Sarbanes-Oxley Act of 2002), el contar con antivirus y parches de seguridad se transformó en una obligación en todas las PCs de los usuarios. Por eso esta tecnología tiene la capacidad de detectar si está presente y activo el antivirus en la máquina y también si las actualizaciones automáticas están activadas. Los agentes se pueden configurar para mandar mensajes periódicamente, y cuando el servidor central no lo recibe manda un alerta al administrador para proceder como fuese necesario. Otro beneficio de este tipo de sistemas es que pueden realizar en forma automática inventarios de hardware consultando el BIOS de la máquina. De esta forma, cuando haya que reemplazar una parte de un equipo, el técnico que tenga que instalar el nuevo dispositivo puede saber exactamente qué modelo de repuesto debe llevar a la oficina del usuario o sucursal remota.

Además de la administración remota del equipo, las placas de Intel equipadas con este sistema permiten agregar características de seguridad, por ejemplo firewalls personales que ejecutan filtros más rápidamente que los que puedan existir instalados sobre el Sistema Operativo. Los administradores tendrían la posibilidad de bloquear determinado tráfico que pueda afectar masivamente a máquinas en presencia de algún virus. Este tipo de firewall se llama "Circuit Breaker", y se implementa en hardware, lo cual hace mucho menos vulnerable al equipo.

Circuit Breaker es un proyecto de investigación de Intel cuyo objetivo es desarrollar la protección de los equipos ante nuevos worms, permitiendo que cada dispositivo monitoree inteligentemente el estado de su propio tráfico de red, y ayuda a confinar el contagio de virus a un grupo reducido de equipos. Ante un ataque masivo se pueden suavizar las consecuencias desde la consola del administrador de IT, y de esta forma drástica proteger a las máquinas más rápidamente.

> "Circuit Breaker es un proyecto de investigación de Intel cuyo objetivo es investigar la protección de los equipos ante nuevos worms"

Conclusión

Ahora los usuarios corporativos móviles podrán tener un mejor servicio de soporte de IT, y desde el punto de vista de la seguridad y administración, el departamento de IT tiene una herramienta poderosa para solucionar problemas rápidamente y con menor costo.●

Centrino Pro

Posee un Procesador Intel® Core™2 Duo, combinado con un Chipset Intel® GM/PM965 o GL960 Express para equipos portátiles.
Cuenta además con Intel® Active Management Technology (AMT) 2.52, permitiendo notables facilidades para administrar los equipos de forma remota y realizar tareas de mantenimiento, y Mobile Intel® Graphics Media Accelerator X3100 (sólo en los chipsets GM965/GL960), ofreciendo un software mejorado capaz de entregar video de alta calidad con un consumo de energía mínimo.
Ofrece además conectividad WLAN, a través de una conexión de red Intel® 82566 Gigabit, y cuenta con Tecnología inalámbrica Intel® Wireless WiFi Link 4965AG PRO/Wireless Network Connection.

Centrino Duo

Posee un Procesador Intel® Core™2 Duo, un procesador dual-core con un Front Side Bus de 800MHz. Además, cuenta con Arquitectura Intel® 64, permitiéndole al usuario sacar ventajas de las aplicaciones de 64-bit a medida que vayan saliendo al mercado.
El poderoso micro se combina con un Chipset Intel® GM/PM965 Express para equipos portátiles, que cuenta con tecnología Intel® Graphics Media Accelerator X3100, transformando al equipo en un poderoso centro multimedia al entregar video de alta calidad y soporte para una experiencia en alta definición.
En términos de conexión inalámbrica, ofrece Intel® Next-Gen Wireless-N e Intel® PRO/Wireless 3945ABG, que permite conectarse a la red a través de infraestructuras LAN 802.11b, 802.11a y 802.11g.

Links Relacionados

http://www.pcworld.idg.com.au/index.php
Inside Intel's Santa Rosa plataform
http://reviews.zdnet.co.uk/hardware/components
Sata Rosa y el Mobile Market
http://www.pcmag.com

Ley de Sarbanes-Oxley
http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Posibilidades de AMT

Detectar

La tecnología de gestión activa de Intel almacena información de hardware y software en la memoria no volátil y permite detectar los activos, incluso cuando los equipos están apagados. Con Intel AMT, las consolas remotas no dependen de los agentes de software locales, contribuyendo así a evitar la pérdida accidental de datos.

Reparar

Intel AMT proporciona funcionalidades de gestión fuera de banda para que el personal de IT pueda reparar los sistemas de forma remota tras los fallos del sistema operativo. Las alarmas y el registro de eventos ayudan al personal de IT a detectar los problemas rápidamente para reducir los periodos de inactividad.

Proteger

Intel AMT ayuda a proteger la red al hacer más fácil mantener el software y la protección contra virus constante y actualizada en la totalidad de la empresa. El software de otras empresas puede guardar los números de versión o los datos de las políticas en la memoria no volátil para recuperaciones o actualizaciones fuera del horario laboral.

¿Se puede hacer Dinero con el Software Libre?

Daniel Coletti
Director de Xtech

El software libre hace rato que está entre nosotros. Inicialmente y por muchos años el software libre fue creado exclusivamente por personas que decidían que al liberarlo (bajo alguna de las licencias que convierten al software programado en software libre) incrementaban las libertades de las personas que lo utilizaban. Como consecuencia de esto el software se distribuía más naturalmente, mejoraba su calidad, seguridad, estabilidad y solidez. Esto aún sigue ocurriendo, pero desde solo hace poco más de una década existen personas (y especialmente empresas) que liberan el software programado porque reconocen que es mejor negocio, que se puede hacer más dinero de esta forma que de la tradicional (el software propietario).

En este artículo voy a mostrar algunas de todas las formas con las que se puede hacer dinero liberando el software o simplemente utilizando el software libre existente (sin programar una línea de código).

Para comenzar es importante entender una premisa: el software libre es, valga la redundancia, libre y no necesariamente gratis.

La forma más fácil de hacer dinero con el software libre es a través de los servicios que se brindan alrededor del software. Por ejemplo: capacitación, soporte y mantenimiento, consultoría e implementación de dicho software en empresas. Este tipo de servicios también existen alrededor de software propietario y en muchas ocasiones, especialmente con software complejo y muy flexible, hay muchísimo más dinero involucrado en los servicios de lo que se gasta en sus licencias de uso.

Actualmente existen muchas empresas que adoptan el modelo de negocios del software libre basado en los servicios, tanto en la Argentina como en otros países del mundo. La mayoría de estas empresas no tienen programadores, son esencialmente empresas que contratan gente que conoce los productos libres desde el punto de vista del usuario, pero con un nivel de profundidad importante. Estos empleados generalmente no saben cómo cambiar el software que implementan, cómo agregarle una funcionalidad nueva, por lo tanto no son tan buenos programadores de este software como lo son como implementadores (o usuarios). A medida que el software libre se sigue propagando existen más y más personas que se convierten en usuarios expertos de cierto software libre, por ende proclives a que estas empresas los contraten o a crear sus propias empresas aumentando más la oferta de este tipo de servicios.

La reacción inicial del empresario que viene trabajando con software propietario (creándolo especialmente) es siempre la misma: ¿Cómo puedo diferenciarme de mi competencia si todo el mundo tiene acceso al mismo software?

En lo que resta del artículo voy a tratar de responder esta pregunta con eficacia.

Capacitación

El servicio de capacitación es el más sencillo de ofrecer en su forma más simple. Solo se requiere una persona idónea en el tema (y un poco de marketing/publicidad) para comenzar a brindar este servicio. Dado que es el servicio más sencillo para comenzar es lógicamente donde hay más competencia. La forma de diferenciarse de la competencia en este tipo de servicio se concentra en mejorar constantemente los temas que se dan, tener buenos docentes (que además de conocer el software sepan explicarlo y capacitar gente), tener buena infraestructura y buen marketing. Por supuesto que todo esto requiere de dinero, pero se puede comenzar con poco ya que el mercado de usuarios está en constante (y rápida) expansión.

Consultoría e Implementación

A mi entender la consultoría es el servicio que se le brinda a las empresas que no conocen las capacidades del software desde un punto de vista macro y general, empresas que requieren de un experto (o varios) que los guíen para poder resolver los desafíos impuestos para mejorar la rentabilidad del negocio de la empresa para la cual trabajan (o la propia). Este servicio requiere de justamente: expertos, personas que comprenden al detalle las problemáticas de una industria en particular (o de varias) y además saben qué tipo de software existe para implementar una solución a estos


“Desde hace más de una década existen personas y empresas que liberan el software programado porque reconocen que se puede hacer más dinero de esta forma que con el software propietario”

problemas o desafíos. Cuanto más y mejores expertos tenga la empresa proveedora y/o pueda demostrar un historial de desafíos similares resueltos exitosamente en otros clientes, más negocio va a tener y lo que es importante, mejores negocios (con más rentabilidad).
Actualmente existe muchísimo software libre para resolver una infinidad de desafíos, si bien no es necesario conocer todas estas aplicaciones, conocer algunas de ellas (las más famosas o las mejores) acabadamente le permite al proveedor diferenciarse fuertemente de sus competidores.
La implementación de este software replica los mismo requerimientos que la consultoría: expertos, pero para diferenciarse de otras empresas que ofrecen los mismo servicios se le agrega la efectividad y velocidad con que se implementa el software (¿acaso Ud. no le pagaría más a una empresa de construcción que puede terminar una casa en un día versus otra empresa que hace lo mismo pero en varios meses? Si la respuesta a esta pregunta es NO es porque Ud. nunca vivió en una casa en construcción).
Adicionalmente, tener buenos procedimientos, buena metodología, control de proyectos, etc. achican las probabilidades de fracaso, pérdidas de tiempo y mejoran ampliamente el resultado final de una implementación entregando informes de resultado y estado de situación final.

Soporte y mantenimiento

Con buenas implementaciones o sin ellas, el servicio de soporte y mantenimiento es un negocio redituable. Entendiendo que la diferencia entre soporte y mantenimiento radica en (soporte) arreglar problemas, (mantenimiento) el servicio de mantener saludable una implementación en producción para evitar que se produzcan problemas, se puede tener diferentes tipos de técnicos para los dos tipos de este servicio.
Los sistemas operativos libres permiten (desde que existe el "telnet") un facilidad increíble de administración remota. Especialmente cuando el software implementado es un software de infraestructura (que no tiene una interacción directa con el usuario final), realizar tareas de soporte y mantenimiento es un servicio sumamente escalable. Un técnico puede hacer mantenimiento de una muy buena cantidad de servidores sin levantarse de su puesto de trabajo (accediendo a ellos por Internet o redes privadas). Adicionalmente existe mucho software de monitoría que generan alarmas basadas en cierta condición de variables, lo que hace que ese mismo técnico no tenga que estar observando el movimiento de cada servidor para detectar un problema en potencia.
De similar forma, solucionar problemas ya existentes es muy factible trabajando en forma remota (aunque en algunas ocasiones, por temas de imagen mayormente, es conveniente trabajar en forma presencial).
Cuando un proveedor realiza una buena implementación, el cliente generalmente no duda a la hora de darle a este proveedor el soporte y mantenimiento de esta implementación realizada también.
Por otro lado, brindar soporte y mantenimiento "de entrada" también es factible. Se requiere un buen marketing, buena imagen y un excelente trabajo comercial para que el cliente nos contrate a nosotros y no a la competencia, pero la realidad es que existen muchas empresas que han decido hacer internamente las implementaciones de software libre. Y generalmente son muchas más de lo que uno imagina, por la misma naturaleza del software libre (todo el mundo tiene acceso a él), es muy común encontrar empresas que ni siquiera el CIO sabía que tenía software libre funcionando dentro de su infraestructura de IT.
En estos casos, combinar soporte y mantenimiento con transferencia de conocimiento a los administradores que hicieron las implementaciones, es un buen diferencial y suma mucho a la hora de convencer al CIO dándole a los técnicos beneficios en su carrera profesional.

"La forma más fácil de hacer dinero con el software libre es a través de los servicios que se brindan alrededor del software"

Desarrollo

Desde el punto de vista del desarrollo existen muchas empresas que ganan dinero mejorando o incrementando las funcionalidades de cierto software libre. Especialmente aquellas empresas que fueron las creadoras de un sistema libre en particular. Uno de los ejemplos de esto es la empresa Sendmail Inc., creadores del servidor de correo (libre) sendmail. Al liberar este software generaron un volumen de usuarios increíble que les permite realizar negocios basados en todos los servicios ya descriptos, pero también concretar negocios que requieran un cambio en la funcionalidad de sendmail. ¿A quién contrataría Ud.? ¿A la empresa que inicialmente desarrolló el software o a otra empresa que aparentemente tiene buenos programadores?

Otras líneas de negocio

Con software libre se puede innovar por la integración, eso quiere decir que fácilmente (y legalmente) uno puede integrar diferentes aplicaciones libres para ofrecer un producto todavía no concebido. Por ejemplo un software que convierta a una PC común en una central telefónica con prestaciones que solo brinda una central telefónica apuntada a grandes empresas.
Conociendo varias aplicaciones libres y también detectando una necesidad de una porción de mercado determinada, se puede invertir en el desarrollo de un producto que simplemente sea el pegamento de varias piezas de software y así venderlo en forma masiva, con poco costo de desarrollo e invirtiendo el dinero en publicidad y marketing.

Conclusiones

El software libre es negocio, para llevarlo adelante hay que profundizar en su ideología y entender cómo llevarlo adelante, hay que tomar ciertos riesgos y animarse a involucrarse con nuevas formas de hacer dinero. Las historias exitosas existen por lo que ya hay varias recetas escritas.
Adicionalmente el software libre, especialmente para empresas que desarrollan software legacy, reduce los riesgos de fracaso o de quiebra, si bien también elimina las posibilidades de convertirse en una empresa monopólica en cierto nicho de mercado, no está la posibilidad de que otra empresa -competidora- y con mucho más poder económico nos aplaste con el lanzamiento de un nuevo producto que hace exactamente lo que hace nuestro producto. ●

Referencias

http://www.dwheeler.com/oss_fs_why.html
http://stephesblog.blogs.com/my_weblog/2007/03/the_best _presen.html
http://www.opensource.org/



La telefonía antes de ser IP ¿existió? Parte 2

Ing. Guido Ottolenghi
Gerente Comercial
Quantum Tecnología

Federico Nan
Socio Gerente **Nantec.net**

Recapitulando un poco lo visto en la edición anterior, la telefonía evolucionó a lo largo de más de un siglo pasando de la transmisión utilizando señales analógicas sobre un medio físico como pares de cobre hasta la conmutación manual de circuitos. Las señales analógicas, a medida que se multiplicaban los enlaces de larga distancia fueron montadas en transportes de radio, o empaquetadas en grupos de canales analógicos por medio de la tecnología FDM, es decir muliplexación por división de frecuencia. Más adelante los canales telefónicos comenzaron a ser digitalizados y transportados en tramas de 30 canales y sus múltiplos, dando paso a la técnica de multiplexación por división de tiempo o TDM.

La señalización, desde niveles y pulsos, pasó a tonos y luego a bits asociados a los canales transmitidos ya sea dentro de la ranura de tiempo asignada al canal o en canales específicos. En ese lapso las redes de datos pasaron desde el telégrafo y el telex transmitidos por pulsos sobre hilos de cobre a ser enviados por FDM, y más adelante por TDM.

La conmutación evolucionó desde sus comienzos, desde manuales a centrales automáticas que utilizaban señalización de pulsos tanto en la interface con el cliente como para las comunicaciones entre centrales (interface de red). Con el tiempo fue apareciendo la señalización multifrecuente entre registros y entre centrales, llegando eventualmente a la interface de cliente, mientras se evolucionaba a través de soluciones electromecánicas cada vez más elaboradas e inteligentes para establecer las llamadas entre dos interlocutores. La conmutación pasó más adelante a disponer de un control electrónico que operaba sobre matrices de relays cada vez más sofisticados, pero que en definitiva aseguraban una conexión galvánica entre entrada y salida utilizando un contacto mecánico con las limitaciones que ello implica. Fue la época de las centrales semielectrónicas. El siguiente paso consistió en la implementación de matrices espacio-temporales, en las que ya no había un camino metálico entre entrada y salida, y que encauzaban los canales muestreados digitalizados y codificados. La operación sobre señales digitales permitía establecer configuraciones y enrutamientos de una manera mucho más flexible. Las centrales digitales permiten brindar una cantidad de servicios adicionales, impensables para centrales electromecánicas y semielectrónicas, desde la indicación de llamada en espera, conferencia, identificación de llamada, rellamada, desvío, casilla de voz, etc.

TECNOLOGIA RDSI (ISDN)

Otra etapa en la evolución fue la introducción de las tecnologías de integración de redes de voz y datos. Las tecnologías de red de servicios integrados (RDSI o ISDN en inglés) prometían un futuro de una red única capaz de transmitir voz y datos indistintamente, unificando la interface de acceso al cliente, que podría conectar diferentes dispositivos según la necesidad y contaría con una gran variedad de servicios adicionales. Los estándares de la ITU ya estaban consolidados a fines de los ´80 para que la industria pudiera ofrecer productos.

FOTO: http://www.sxc.hu/ - Pawel Zawistowski



La tecnología RDSI tuvo una significativa aceptación en algunos países, especialmente en Europa, mientras que en USA no logró atraer tanto la atención del mercado tal vez porque las operadoras telefónicas no pusieron énfasis en educar al consumidor en cuanto a los beneficios y sobre todo en cuanto a cómo implementar y configurar los equipos asociados al servicio en su red interna. En Sudamérica el despliegue de RDSI es muy limitado o nulo en algunos países. Ya sea por cuestiones regulatorias o de falta de actualización tecnológica y/o justificación de las inversiones, esta tecnología se desplegó en pocos países y en forma limitada a empresas fundamentalmente interesadas en comunicarse con interlocutores en países europeos o USA y realizar video conferencias.

La RDSI utiliza principalmente dos tipos de acceso, el Básico (BRI) y el Primario (PRI), el primero compuesto de dos canales B de 64 kbps cada uno, para transmisión de voz y/o datos, y un canal D de 16 kbps para señalización y transmisión de datos a baja velocidad. El acceso Primario, en cambio, utiliza una trama de 2 Mbps en la que configura 30 canales B y un canal D en este caso de 64 kbps. Otras definiciones de canales son H0 (384 kbps), H11 (1536 kbps) y H12 (1920 kbps) concebidos para brindar servicios que requieran mayor ancho de banda que el provisto por un acceso Básico.

Por su parte, las redes de datos habían evolucionado inicialmente aprovechando la infraestructura de la red telefónica. Varios factores impulsaron el crecimiento de las redes de datos, entre ellos la evolución de la tecnología informática.

Inicialmente, las computadoras eran de gran porte y extremadamente costosas, lo que alentó el uso compartido de sus recursos. Entre las formas de utilización compartida el de las terminales remotas requería el uso de una red de comunicaciones. Las terminales remotas se comunican vía la red telefónica utilizando modems.

A pesar del mejoramiento progresivo de las tecnologías de modems el uso de la red telefónica para estas aplicaciones era ineficiente principalmente porque el circuito se establece en forma permanente pero se transmiten datos cada tanto y no necesariamente en ambas direcciones en forma simultánea.

Además del teleprocesamiento, utilizado para sistemas bancarios, reservas de pasajes y otras aplicaciones, surgieron otras prácticas como la telemática dentro de la que se incluían por ejemplo las compras por catálogo, sistemas EDI (Electronic Data Interchange) que requerían la interconexión de terminales y computadoras a través de grandes distancias. La reducción de costos de los equipos informáticos facilitó su difusión y con ello el incremento exponencial de las necesidades de una infraestructura de comunicaciones apropiada. Todo esto impulsó el desarrollo de las redes de conmutación de paquetes. Los datos a transmitir son fragmentados en paquetes de cierta longitud que contienen una porción de los datos e información adicional para el correcto encaminamiento del paquete. De esta forma, los paquetes son encaminados a través de una serie de nodos de conmutación para llegar a destino, en forma similar a lo que ocurre con el encaminamiento de una llamada telefónica. Sin, embargo, a diferencia de lo que ocurre con ésta, en el caso de las redes de conmutación de paquetes, éstos son recibidos por un nodo y encaminados hacia el siguiente utilizando un enlace compartido con otros paquetes que deben ser encaminados por esa misma "pierna" de la red. Ese paquete dispone del recurso que es parte de la capacidad del enlace entre esos dos nodos solamente cuando debe ser transmitido. No hay por lo tanto una asignación permanente en el tiempo de una porción del recurso para esa transmisión.

Cada paquete, por lo tanto, lleva consigo información necesaria para llegar a destino, y, en base a la disponibilidad de recursos, en cada nodo puede ser retransmitido inmediatamente o almacenado a la espera de que el siguiente enlace tenga capacidad disponible.

El beneficio de un mejor aprovechamiento del vínculo tiene que pagar el precio del riesgo de congestión. En el caso de las redes de conmutación de circuitos puede haber bloqueo, es decir no se puede establecer la comunicación, si la demanda de tráfico supera la capacidad de una parte de la misma. Un ejemplo típico hasta principios de los ´90, en Argentina y en una red de conmutación de circuitos como es la red telefónica, era descolgar el teléfono y no recibir tono, o marcar el número y al tercer dígito recibir señal de ocupado.

Una vez establecido el enlace, el canal está disponible, se use o no. En el caso de la conmutación de paquetes, puede haber congestión en algún nodo retrasando o impidiendo la transmisión de paquetes a través de uno o más nodos. Si la congestión persiste es posible que se exceda la capacidad de almacenamiento de paquetes del nodo y se pierdan paquetes que deban ser retransmitidos más tarde. De hecho la gestión de situaciones de congestión es un aspecto de la mayor importancia en estas tecnologías. El estándar más conocido y utilizado como interface en una red de conmutación de paquetes y un terminal es el X.25, que se emplea para conmutación de paquetes en ISDN. El estándar cubre tres niveles de protocolos, a saber: el físico, el de enlace y el de paquetes que corresponden a los tres niveles más bajos del modelo OSI.

Los datos de usuario son sucesivamente anexados a un encabezado de capa 3 convirtiéndose de esta forma en un paquete X.25, y el conjunto encapsulado con un header y trailer LAPB que da origen así a una trama LAPB (Link Access Protocol Balanced). El LAPB es un subconjunto del HDLC (High Level Data Link Control). El LAPB evolucionó al LAPD posteriormente.

En una red de conmutación de paquetes pueden considerarse dos modalidades de transmisión, una basada en Datagramas en la que cada paquete es tratado independientemente con relación a los paquetes precedentes, y la

FOTO: http://www.sxc.hu/ - Pawel Zawistowski



otra basada en Circuitos Virtuales, en que se preplanifica una ruta antes de enviar los paquetes. A su vez, cada modalidad se puede aplicar a la interface usuario red (servicio externo) y a la operación interna dando así lugar a 4 combinaciones posibles. De estas combinaciones, la que emplea Circuitos Virtuales externa e internamente es la que establece una ruta previa al envío de paquetes. En el caso de datagramas, en la fase externa e interna, cada paquete es tratado independientemente. El eventual reordenamiento de paquetes que pueden llegar por diferentes rutas cada vez o la recuperación de paquetes perdidos queda a cargo de niveles superiores. En el caso de Circuito Virtual externo y Datagrama interno, es la red la que debería proveer los recursos para reordenar los paquetes una vez recibidos de las diferentes rutas que pueden establecerse. La cuarta alternativa, Datagrama externo y Circuito Virtual interno desaprovecharía el valor adicional de disponer de un Circuito Virtual en la fase interna.

La elección del tipo de modalidad depende del objetivo de diseño de la red y los costos involucrados. En la práctica, el servicio basado en circuitos virtuales es mucho más común que el de datagramas. Este es apropiado para aplicaciones en tiempo real que utilizan la red en forma eficiente por no requerirse el setup de la comunicación ni la retransmisión de paquetes perdidos.
A medida que los requerimientos de volumen de datos fueron empujando los límites de velocidad emergieron otras tecnologías de conmutación de paquetes que, aprovechando la confiabilidad de las redes y los enlaces de transmisión, prescindieron de los aspectos relativos al control de errores delegándolos a las capas superiores.

FRAME RELAY

Frame Relay es una de estas tecnologías que pasó a manejar velocidades a nivel de usuario del orden de los 2 Mbps frente a las redes de conmutación de paquetes originales que en cambio manejaban velocidades del orden de 64 kbps. En las redes X.25 hay un considerable overhead debido a los paquetes de control de llamada que establecen y desconectan los circuitos virtuales, el multiplexado de circuitos virtuales que ocurre en la capa 3 y el control de flujo y control de errores en capas 2 y 3. Este overhead puede justificarse en contextos de tasas de error de bits relativamente altos. Al mejorar la confiabilidad de los enlaces se puede omitir sin desmedro de la integridad de la comunicación siempre y cuando esa menor cantidad de errores puedan ser manejados por los protocolos de nivel superior. El resultado es una estructura más "liviana" que provee una mayor capacidad de transmisión a costos razonables.

ATM

Así como Frame Relay es una tecnología que surgió de los trabajos de normalización de ISDN, ATM es un producto resultante de los trabajos de normalización de ISDN de Banda Ancha. A mediados de los 80, cuando se iniciaron tareas de definición de estándares relacionados con B-ISDN (ISDN de Banda Ancha) se asumió en general que se utilizaría como transporte alguna técnica TDM sincrónica como en el caso del acceso Básico Primario de ISDN de banda angosta.
Sin embargo, el enfoque de una solución sincrónica tiene varios inconvenientes, entre los que vale la pena mencionar que no dispone de una interface flexible que cumpla con la variedad de necesidades previsibles a partir de las aplicaciones que utilizarían esa tasa de bits tan alta. El esquema que se discutía en ese momento era el de formar estructuras que permitieran combinaciones de canales B, Hi y un canal D de control.
La perspectiva de contar con una variedad discreta de velocidades por medio de la agregación de canales de una variedad de velocidades permitía vislumbrar un aprovechamiento ineficiente de los recursos. Por otra parte, hay datos que son de naturaleza intempestiva que requerirían un gran ancho de banda en ciertos momentos y poco o nada en otros. Este aspecto y la granularidad mínima de 64kbps de los canales TDM fueron dos factores adicionales que indujeron a considerar otras opciones. Finalmente, el esquema basado en señales de múltiples velocidades iba a incrementar la complejidad de los nodos de conmutación que debían adaptarse a una variedad de velocidades pautadas mientras que hasta entonces manejaban exclusivamente flujos de 64 kbps.
Conceptualmente ATM es similar a Frame Relay. Ambos descansan en la confiabilidad de la infraestructura de red existente para brindar el servicio de conmutación de paquetes. ATM maneja velocidades mayores. También soporta múltiples conexiones lógicas sobre un mismo medio. Estas conexiones se implementan por medio de un flujo de paquetes de tamaño fijo de 53 bytes llamados celdas y que están compuestos por 5 bytes de encabezado y 48 de información.
El encabezado da cuenta del VPI, VCI los identificadores de camino (path) y canal con los que se designan las conexiones lógicas, y otras informaciones como el tipo de datos que transportan, la prioridad que da una indicación de cuán descartable es la celda en caso de congestión, y el control de error de encabezado que se utiliza para control de error y sincronización.

La ventaja de utilizar un esquema de caminos y canales virtuales en contraste con los circuitos virtuales propios de X.25 reside en la mayor facilidad de gestionar canales en base a un mismo origen y destino y el de asignar servicios y otros condicionamientos en base al agrupamiento.
La integración de los flujos en celdas de tamaño relativamente chico permite asignar ancho de banda con una granularidad imposible de obtener por métodos sincrónicos, inclusive hacer dinámica la asignación para responder a demandas intempestivas e irregulares de ciertas aplicaciones. En este punto puede ser conveniente señalar que la evolución tecnológica fue orientándose con el objetivo de optimizar el aprovechamiento de los recursos ante la creciente necesidad planteada por los usuarios de disponer de más servicios y más ancho de banda a costos razonables.
Las tecnologías que terminan imponiéndose son las que brindan las mejores posibilidades al mercado, y la adopción por parte del mismo es lo que consolida la prevalencia por el efecto de masificación que baja los costos, multiplica las alternativas y diversifica las aplicaciones. Es así que, mientras una parte de la industria evoluciona por los tradicionales procesos de los sólidos y corpulentos estándares de la ITU, otras tecnologías surgidas del ámbito de investigación y concebidas originalmente para la defensa, y otras más, desarrolladas para la LAN se expanden a la WAN por esta combinación de efectos, superponiéndose y complementándose con las "históricas".

Junto con el ascenso de ATM se dieron otras tecnologías y circunstancias que orientaron el mercado hacia otras soluciones que en el próximo capítulo investigaremos. ●

Escritorios 3D en GNU-Linux

Hoy en día se están empezando a poner de moda los escritorios tridimensionales; y aunque para muchos esto es algo nuevo, lo cierto es que los usuarios de Gnu-Linux hace más de un año que los vienen disfrutando. En esta nota les contaremos el futuro de esta maravilla 3D.

■ Leonel Iván Saafigueroa

Un poco de historia

Esta revolución del escritorio 3D comenzó gracias al gran aporte de Novell (compañía estadounidense ubicada en el valle de Utah), dedicada a la creación de software en el área de redes y conocida por productos como: Novell Netware y Linux (siendo dueña de los derechos de la distribución Suse Linux).

Fue en enero del 2006 cuando presentó "Compiz", su gestor de ventanas de composición para el sistema "X Window", el mismo era capaz de aprovechar la aceleración OpenGL con una integración que le permitía realizar efectos como: minimización y una vista del espacio de trabajo en forma de cubo.

Siguiendo los estándares ICCCM, "Compiz" podía ser sustituto de los gestores por defecto de GNOME (Metacity), KDE (KWIN) y XFCE4.

"Beryl" - El fork de la gran comunidad

Cuando un grupo de personas que trabajan en un proyecto en común empiezan a tener ideas distintas, lo más probable es que se decida seguir cada grupo por su lado, creando de esta manera una ramificación ("Fork") del proyecto original y dando comienzo a uno nuevo; en el mundo del software libre es algo muy común (sucedió antes con Xfree, dando como resultado el actual X.org).

Esto fue lo que sucedió también con Compiz, debido a preferencias personales y a diferencias técnicas, el 19 de septiembre del 2006 se realizó un anuncio



Fig. 1 CTRL+TAB nos permite cambiar de aplicación

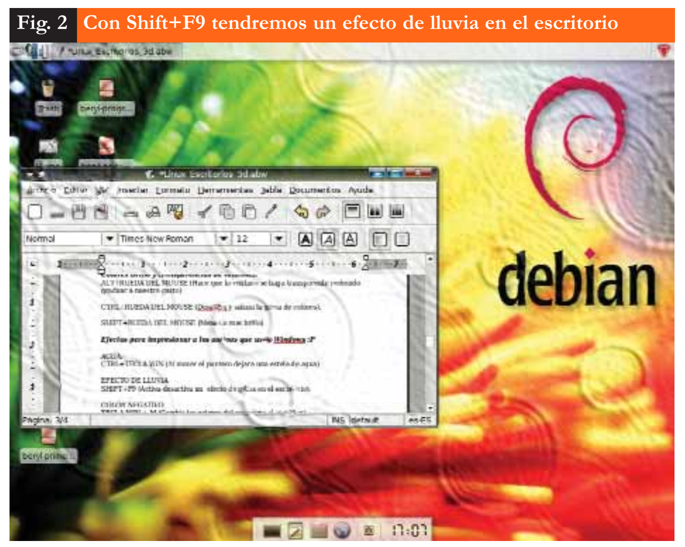


Fig. 2 Con Shift+F9 tendremos un efecto de lluvia en el escritorio

Analizamos "Beryl" el administrador de Ventanas 3D



Fig. 3 Escritorio Debian XFC4 girando el cubo



Fig. 4 Miniaturas de todas las aplicaciones abiertas

en el foro de Compiz.net, indicando que la ramificación de Compiz (Compiz-QuinnStorm) mantenida por la comunidad se mudaría a un proyecto llamado "Beryl". Este Fork incluía un conjunto de plugins, patches, y aplicaciones que hacían de "Beryl" un producto muy superior al proyecto de Novell, con sustitutos completos para la configuración y decoración de las ventanas.

Sistemas soportados por "Beryl"

Actualmente podemos encontrar "Beryl" (muchas veces de forma no oficial) para Fedora, Debian, Mandriva, Suse. Incluso en el nuevo Ubuntu Desktop 7.04 "Feisty Fawn", una vez instalado, podemos activar "Beryl" desde el administrador de paquetes; de este último Ubuntu podemos pedir una copia y nos lo enviaran gratuitamente por correo (https://shipit.ubuntu.com/).

También hay muchas distribuciones Live Cd, con las cuales podremos probar el escritorio 3D sin necesidad de reemplazar nuestro actual sistema operativo, pues se ejecuta completamente desde el CD-Rom.

Otro modo es bajando el código fuente desde la página del proyecto, en teoría cualquier sistema Gnu-Linux es apto para poder integrar "Beryl".

Requerimientos de Hardware

Inicialmente Compiz sólo funcionaba en los tipos de hardware soportados por Xgl (la mayoría de las tarjetas gráficas NVIDIA y ATI trabajan en Compiz sobre Xgl), pero es posible encontrar errores tanto en Xgl como en Compiz, ambos sistemas son casi nuevos y aún están en pleno desarrollo.

Los drivers de las tarjetas NVIDIA (desde la Versión 1.0-9625 BETA) soportan la extensión GLX_EXT_texture_from_pixmap de la norma X.Org server, por lo cual funciona bastante bien.

Para instalar XGL + beryl, básicamente es necesario una tarjeta que permita la aceleración gráfica, en Internet muchos comentan que en un Pentium III de 800 Mhz se ejecuta perfectamente; con tarjetas gráficas antiguas como la Ge Force 2 de Nvidia, o con tarjetas Intel (muchas veces integrada) funciona sin problemas, no es necesario tener una máquina tan potente para hacer la prueba.

El futuro del escritorio 3D se llamará "Compiz Fusion"

Actualmente los proyectos Beryl y Compiz se han unido para formar un proyecto en común (dicen que la unión hace la fuerza). En un principio el nuevo proyecto fue bautizado con el nombre en código "CompComm", al menos hasta que se decidieran por alguno de todos los posibles nombres, entre ellos: Blitz, Cobalt, CoCo, Coral, Fusion y Nova.

Finalmente el pasado 20 de junio gracias a una encuesta que se llevó a cabo en los foros de discusión del proyecto conjunto, los desarrolladores más activos han decidido llamar al proyecto Fusion; siendo "Compiz" el core (o núcleo) y "Fusion" las animaciones, plugins y extras; por lo tanto, a partir de ahora los dos proyectos se convierten definitivamente en uno con el nombre "Compiz Fusion".

Aun falta elegir cual será el nuevo logo del proyecto, aunque quieren organizar un concurso para su diseño.

Muchas mejoras se esperan de esta unión, y ya es posible encontrar en Internet las versiones de prueba de "CompComm", los dos proyectos añadían una serie de increíbles efectos visuales al escritorio de Linux. "Compiz Fusion" es algo que escucharemos con mucha frecuencia desde ahora pues de seguro nos sorprenderá con sus nuevos e increíbles efectos.

Origen del nombre Beryl

Beryl viene del "Berilio", elemento químico de símbolo BE, el cual se encuentra en diversas piedras preciosas, entre ellas: el diamante, el rubí, la amatista, la aguamarina, y la esmeralda. Todas estas piedras se extraen habitualmente de canteras sudamericanas, en países como Brasil, Bolivia, y en el norte de Argentina, son conocidas por su belleza y valor económico.

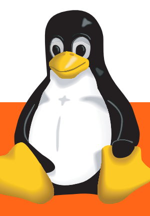
Páginas de Internet

- Página oficial del proyecto Compiz:
http://www.compiz.org/

- Página oficial del proyecto Beryl:
http://www.beryl-project.org/

- Beryl-Themes
(Distintos diseños de ventanas):
http://themes.beryl-project.org/

- Página oficial de la unión Compiz-Beryl:
http://www.opencompositing.org/



¿Es necesario instalar GNU-Linux para probar un escritorio 3D?

Si realmente tienes curiosidad de ver cómo funciona un escritorio 3D en Gnu-Linux, puedes probar "Uberyl" (buntu + beryl). Es capaz de correr beryl en modo live-cd con Intel, Nvidia & Ati. Lleva instalado Songbird, Automatix, Envy, Emulators , Xara xtreme, youtranslator, Avant window navigator, apton-cd, ndiskgtk (wireless drivers tools).
Lo puedes descargar desde aquí: *http://uberyl.avefenix.es/*

Conclusiones

La mayoría de los usuarios de Gnu-Linux son elitistas, gustan de los escritorios sencillos y ahorran todos los recursos de memoria y procesador que puedan.

Muchos califican a Compiz y Beryl como meras mejoras visuales que apenas aportaban funcionalidad práctica alguna; otros creen que contar con un escritorio más vistoso es importante.

Microsoft y Apple han incluido muchas mejoras visuales también en sus últimos sistemas operativos, pero Gnu-Linux demuestra que no es necesario tener una máquina tan potente y en muchas ocasiones costosas para igualar o mejorar las interfaces gráficas del usuario.

Solo resta esperar qué nos depara el futuro con "Compiz Fusion", ya nos demostraron qué son capaces de hacer, ahora es cuestión de verlo mejorar cada día en las manos de la comunidad del Software Libre. ●

Sobre el autor:

Leonel Iván Saafigueroa
Es analista de Sistemas, docente, radioaficionado (LU5ENP) y conductor del programa de radio libre hispano - Red-Handed Radio (www.red-handed-radio.com.ar)

Atajos de teclas usadas en Beryl

Combinando ciertas teclas y también con ayuda del mouse, podremos manejar este increíble escritorio 3D de forma práctica:

Hacer girar el cubo:
CTRL+ALT+FLECHA DERECHA/IZQUIERDA (Gira el cubo hacia la derecha o izquierda respectivamente).

CTRL+ALT+BOTON IZQUIERDO DEL RATON (Podremos girar el cubo libremente moviendo el mouse).

Cambio de aplicación:
ALT+TAB (Cambia entre las ventanas del espacio de trabajo actual; cara actual del cubo).

CTRL+ALT+TAB (Cambia entre ventanas de todos los espacios de trabajo; todas las caras del cubo).

F9 (Muestra miniaturas de todas las ventanas abiertas en el espacio de trabajo actual o cara actual del cubo, y nos permite elegir cualquiera).

F8 (Muestra miniaturas de todas las ventanas abiertas, y nos permite elegir cualquiera.)

PUNTERO EN LA ESQUINA SUPERIOR DERECHA (Al igual que F8, muestra miniaturas de todas las ventanas abiertas, y nos permite elegir cualquiera).

ALT + BOTON IZQUIERDO DEL MOUSE (Movemos la ventana para ver que hay detrás).

Colores, brillo y transparencias de ventanas:
ALT+RUEDA DEL MOUSE (Hace que la ventana se haga transparente pudiendo graduar a nuestro gusto).

CTRL+RUEDA DEL MOUSE (Desatura y satura la gama de colores).

SHIFT+RUEDA DEL MOUSE (Menos o más brillo).

Efectos para impresionar a los amigos que usan Windows :P

Agua:
CTRL+TECLA WIN (Al mover el puntero dejara una estela de agua).

Efecto de lluvia:
SHIFT+F9 (Activa-desactiva un efecto de gotas en el escritorio).

Color negativo:
TECLA WIN + M (Cambia los colores del escritorio al negativo).

Color negativo:
TECLA WIN + N (Cambia los colores de la ventana actual al negativo).

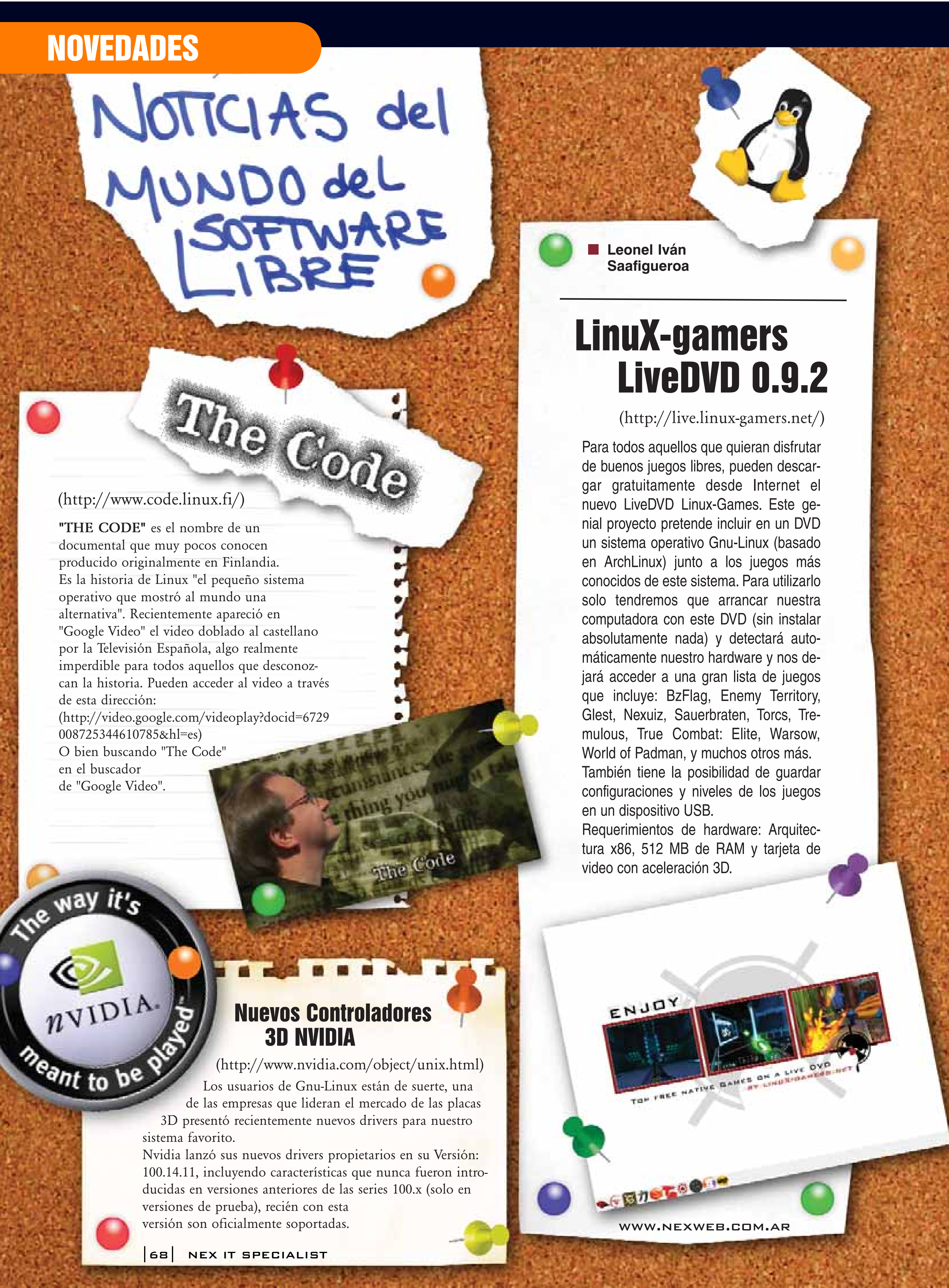
Zoom:
TECLA WIN + RUEDA DEL RATON (Podremos ajustar el zoom de la pantalla a nuestras necesidades).



Fig. 5 Distintas aplicaciones en las caras del cubo



Fig. 6 Miniaturas de todas las aplicaciones de una cara del cubo



Noticias del Mundo del Software Libre

The Code

(http://www.code.linux.fi/)

"THE CODE" es el nombre de un documental que muy pocos conocen producido originalmente en Finlandia.
Es la historia de Linux "el pequeño sistema operativo que mostró al mundo una alternativa". Recientemente apareció en "Google Video" el video doblado al castellano por la Televisión Española, algo realmente imperdible para todos aquellos que desconozcan la historia. Pueden acceder al video a través de esta dirección:
(http://video.google.com/videoplay?docid=6729008725344610785&hl=es)
O bien buscando "The Code" en el buscador de "Google Video".

Nuevos Controladores 3D NVIDIA

(http://www.nvidia.com/object/unix.html)

Los usuarios de Gnu-Linux están de suerte, una de las empresas que lideran el mercado de las placas 3D presentó recientemente nuevos drivers para nuestro sistema favorito.
Nvidia lanzó sus nuevos drivers propietarios en su Versión: 100.14.11, incluyendo características que nunca fueron introducidas en versiones anteriores de las series 100.x (solo en versiones de prueba), recién con esta versión son oficialmente soportadas.

Leonel Iván Saafigueroa

LinuX-gamers LiveDVD 0.9.2

(http://live.linux-gamers.net/)

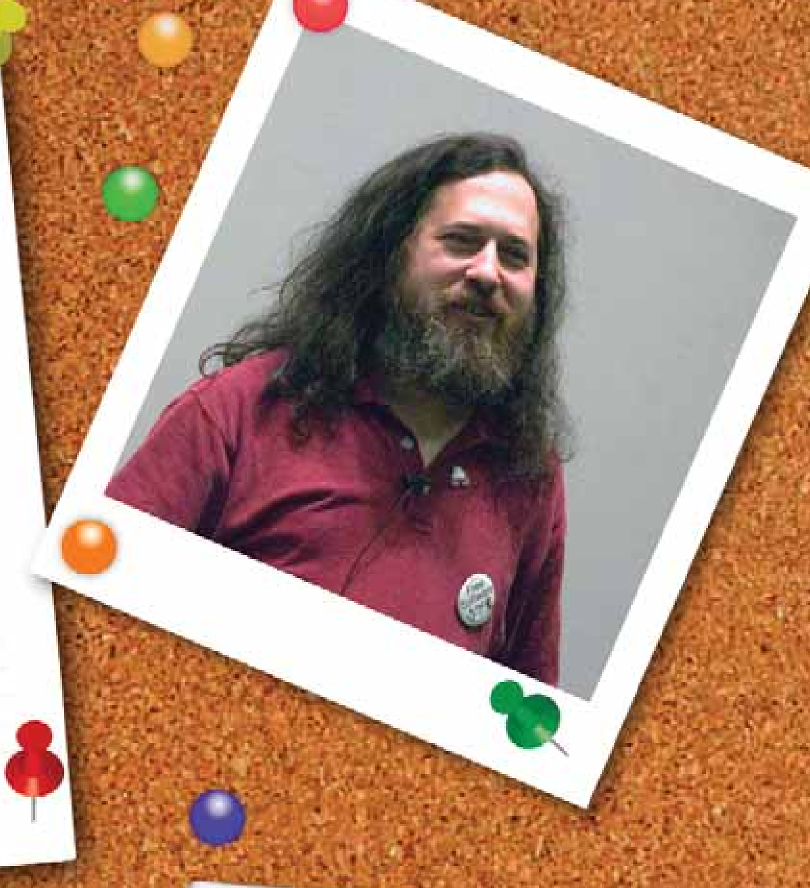
Para todos aquellos que quieran disfrutar de buenos juegos libres, pueden descargar gratuitamente desde Internet el nuevo LiveDVD Linux-Games. Este genial proyecto pretende incluir en un DVD un sistema operativo Gnu-Linux (basado en ArchLinux) junto a los juegos más conocidos de este sistema. Para utilizarlo solo tendremos que arrancar nuestra computadora con este DVD (sin instalar absolutamente nada) y detectará automáticamente nuestro hardware y nos dejará acceder a una gran lista de juegos que incluye: BzFlag, Enemy Territory, Glest, Nexuiz, Sauerbraten, Torcs, Tremulous, True Combat: Elite, Warsow, World of Padman, y muchos otros más.
También tiene la posibilidad de guardar configuraciones y niveles de los juegos en un dispositivo USB.
Requerimientos de hardware: Arquitectura x86, 512 MB de RAM y tarjeta de video con aceleración 3D.



Publicado el cuarto borrador de la GPL 3.0

(http://www.fsf.org/)

La Free Software Foundation, piedra fundamental de todo el movimiento GNU, es una organización internacional dedicada a la promoción y defensa del uso del Software Libre iniciada por Richard Stallman. Recientemente anunció la disponibilidad del cuarto y último borrador de la tercera versión de la GNU Public License.
En esta nueva versión se destaca un apartado que se refiere a la compatibilidad con otras licencias, como por ejemplo la versión 2 de la licencia Apache. También se aclara en qué forma se puede contratar una modificación privada de un Software Libre.
Seguramente para la publicación de esta revista ya estén anunciando la versión definitiva de este documento.





Musix 1.0 Release 1

(http://www.musix.org.ar/)

Musix es el resultado del trabajo colaborativo de toda una comunidad de usuarios y programadores que dieron origen a un Sistema Operativo Multimedia 100 por ciento libre destinado a: músicos, técnicos sonidistas, DJs, cineastas, diseñadores gráficos y usuarios en general. Incluye una enorme colección de programas libres y el mismo se puede iniciar desde una unidad de CD/DVD y es completamente funcional, sin necesidad de instalar nada en el disco duro aunque también puede ser instalado posteriormente.
Musix puede utilizarse en diferentes idiomas: castellano, gallego, catalán, euskera, inglés, portugués, francés, alemán e italiano, y prometen soportar más idiomas en el futuro.
Pueden descargarlo desde su página de Internet.

Slackware 12.0 RC1

(http://www.slackware.org/)

Patrick Volkerding, líder de proyecto Slackware Gnu-Linux, anunció el primer Release Candidate de la versión 12.0 de su popular distribución.
Esta distribución GNU/Linux está orientada a usuarios con cierta experiencia, y se caracteriza por ser desde siempre una de las más estables.
Slackware 12.0 es una enorme actualización que incluye por primera vez un Kernel 2.6 por defecto (2.6.21.5) compilado con GCC4 (4.12), pero también otras novedades como ser KDE 3.5.7, XFCE 4.4.1, Apache 2.2 con PHP 5, y finalmente X.Org 7.2 modular con soporte de Xgl y Compiz.
Aun no hay ninguna imagen ISO oficial para descargar, pero es bueno estar atentos y revisar el servidor FTP donde se publica frecuentemente un ISO no oficial de los últimos cambios en el árbol de desarrollo de Slackware.





Seguridad por CAPAS

Restableciendo una red confiable

El desafío de mantener segura la red

Aunque los problemas principales de la seguridad de una red han cambiado muy poco en la última década, el panorama general se ha modificado de forma drástica. Hoy en día los profesionales de IT todavía tienen la responsabilidad de proteger la confidencialidad de la información de la empresa, previniendo el acceso de gente no autorizada y defendiendo a la red de posibles ataques, aunque también se enfrentan a nuevos desafíos al operar en el complejo y dinámico mundo de la seguridad de la red.

• **Acceso generalizado a Internet:** El acceso a Internet desde diferentes dispositivos ha convertido a cada casa, oficina o partner de negocios en un potencial punto de entrada de los ataques. Este acceso generalizado expone a la red empresarial a ataques sofisticados que pueden ser lanzados por algún hacker o por un usuario remoto que al "logearse" a la red corporativa permita un ataque de tipo "piggy-back". La moda de trabajar en casa y de usar la PC del trabajo para usos personales aumenta la posibilidad de ataques como Spyware, Phishing o SPAM, por lo que este problema debe ser tratado al nivel de la red corporativa. Un estudio realizado en 2005 por el CSI del FBI dio a conocer que el 65 por ciento de las empresas auditadas sufrieron algún ataque de una fuente externa.

• **Ataques internos:** Mientras que frenar los ataques externos representa un desafío constante, igualmente de difícil y engorroso resulta defenderse de los ataques perpetuados desde adentro de la red por empleados que tienen acceso y control total de los recursos de la red. Los ataques internos van desde el acceso a los recursos hasta la destrucción o robo de información delicada.

• **Regulatory compliance:** Sarbanes-Oxley, GLBA, BASEL II y HIPAA son algunas de las diferentes regulaciones con las cuales las compañías deben cumplir y las cuales complican un poco más el trabajo del administrador de la seguridad.

• **Cambiando los niveles de acceso:** Una gama cada vez más extensa de acceso a la red se concede a empleados y no empleados, volviendo más vulnerable la red. Los empleados remotos, partners de negocios, clientes y proveedores pueden tener diferentes niveles de acceso a los recursos de la empresa, por lo que se deben tomar las medidas adecuadas para proteger la red empresarial. Mientras que aumentan las aplicaciones a las que los usuarios remotos tienen acceso a través del DMZ, las compañías tratan de reducir los costos minimizando las aplicaciones entre usuarios internos y externos, lo que hace necesario acomodar las aplicaciones usadas por ambos grupos.

Componentes de la Layered Security Solution

Security Layer	Descripción
Virtual Private Network (VPN)	Protege las comunicaciones entre los sitios y/o los usuarios con una sesión encriptada y autenticada.
Network Firewall	Protege la red mediante el control de quién y qué tipo de acceso a la red tiene cada persona. Detiene el tipo de ataque llamado Denial of Service (DoS).
Intrusion Prevention	Combinación de protección que detecta y frena los ataques al nivel de las aplicaciones.
Antivirus	Protección contra los ataques de virus en el Desktop, en la entrada y a nivel de servidor.
Web Filtering	Frena a los usuarios de visitar páginas web inapropiadas o bajar Spyware u otra aplicación maliciosa desde sitios desconocidos.
Anti-Spam	Reduce la cantidad de correo no deseado.

Solución de Seguridad en Capas (Layered Security Solution)

Los analistas de industrias y los expertos en seguridad coinciden en que la clave para encontrar un balance entre la seguridad de la red restrictiva y el acceso que necesitan los empleados, partners de negocios y clientes es una Solución de Seguridad por Capas (Layered Security Solution).

Esta solución le da al departamento de IT un completo conjunto de herramientas que se pueden utilizar para alcanzar la seguridad end-to-end desde el sitio remoto hasta el data center. La solución está diseñada para proteger los recursos críticos de la red. Si falla una capa, la siguiente detendrá el ataque o disminuirá el daño que pueda provocar.

FOTO: http://www.sxc.hu/ - Natalie Souprounovich

Componentes de la Solución Networks Layered Security de Juniper

Es un hecho aceptado que las intrusiones y los ataques son inevitables y que las estrategias de seguridad por capas compuestas de múltiples tecnologías complementarias de seguridad, todas trabajando en forma conjunta, ayudan a minimizar el riesgo al interponer múltiples barreras entre el atacante y su objetivo. Esta estrategia también le da al administrador de redes más tiempo para reaccionar y evitar mayores daños una vez que el ataque ya ocurrió.

La línea de productos de FW/IPSec VPN de Juniper Networks le da al departamento de IT un completo rango de dispositivos de seguridad de alta performance diseñados para soportar las variadas situaciones que los clientes requieren. Stateful firewall, IPS integrados, mitigación DoS e IPSec VPN son las características estándar de toda plataforma. Además, la plataforma de SSG Family puede ser implementada con un completo e integrado conjunto de características de la seguridad llamado Unified Threat Management (UTM). Con ellas, las empresas pueden desarrollar soluciones por capas para proteger a los usuarios y sitios remotos, a las oficinas regionales y al perímetro de red así como al data center de la red.

Firewall: control de acceso y autenticación

El firewall actúa como la primera capa de la seguridad controlando quién o qué tiene acceso a la red. El firewall de Juniper Networks realiza una inspección de estado (stateful inspection) para proteger a la red del contenido malicioso. Con esta inspección se recoge información de las sesiones TCP y UDP como la dirección IP de la fuente y del destinatario, el número de puerto de la fuente y del destinatario y los números de secuencia del paquete y se mantiene esta información para analizar el tráfico en un futuro.

Control de acceso de usuarios y autenticación

Para un control más completo, el firewall de Juniper, cuando es utilizado como parte de la solución de Unified Access Control (UAC), puede hacer que las políticas avanzadas permitan o nieguen el acceso a los recursos y aplicaciones sobre la identidad de los usuarios y la información de la red.

Segmentación de la red y contención del usuario

En vez de implementar un firewall diferente para cada segmento de la red, el firewall integrado de Juniper Networks brinda una solución más efectiva -la posibilidad de usar un solo dispositivo para múltiples firewalls es una de las dos formas posibles: interfaces físicas y segmentos virtuales.

Protección a ataques de DoS

La solución de seguridad integrada de Juniper Networks puede ser configurada para protegerse de hasta 30 ataques diferentes, tanto internos como externos, incluyendo ataques SYN flood, UDP flood y Port Scan.

Intrusion Prevention

Los ataques a nivel de aplicación son cada vez más comunes y más fáciles de propagar, por lo que es necesario implementar adecuados niveles de protección en los sitios remotos, tanto en el perímetro como en el core de la red.
Para tratar estas cuestiones y lograr aplicaciones de niveles avanzados para la detección y prevención de ataques, la línea de soluciones de seguridad de Juniper Networks brindan dos opciones IPS: Intrusion Detection and Prevention y Deep Inspection Firewall.

> "La Layered Security Solution le da al departamento de IT un completo conjunto de herramientas para alcanzar la seguridad end-to-end desde el sitio remoto hasta el data center"

Juniper Networks IDP

En implementaciones de gran velocidad la protección de las aplicaciones está a cargo del Juniper Networks Intrusion Detection and Prevention (IDP), el cual puede estar implementado de forma independiente o como aplicación integrada de FW/VPN/IDP bajo la Serie ISG (ISG 2000 y ISG 1000).
La información de la red reunida por Juniper Networks IDP incluye ítems como direcciones IP/MAC y número de puerto, mientras que la información de los niveles de aplicaciones incluyen temas como aplicaciones usadas sobre la red, número de versión, nombre de usuario y URL.

Opciones de implementaciones de IDP: integradas o autónomas

Para perímetros de alta velocidad y redes internas donde una solución integrada es la solución, se puede actualizar el Juniper Networks ISG 2000 y el ISG 1000 (Serie ISG) para correr el mismo software IDP en el dispositivo autónomo. Usando la aceleración de hardware de hasta 3 módulos de seguridad, cada uno con su propio procesador y memoria, la serie ISG puede entregar hasta 2 GB/s de IDP para proteger los entornos de alta velocidad.

Deep Inspection Firewall

En locaciones perimetrales y redes, el firewall de Inspección Profunda entrega la funcionalidad IPS, el cual integra las tecnologías de intrusion prevention para determinar si se acepta o no aplicaciones a nivel de tráfico y ataques.
Implementado en el perímetro, IPS hace foco en prevenir los ataques de protocolos controlando su conformación y extrayendo información de los "service fields" desde donde los ataques son perpetuados.

Virtual Private Networks

La siguiente capa de protección utiliza una Virtual Private Network (VPN) para encriptar las comunicaciones que atraviesan un medio poco confiable como Internet o un segmento interno de la red. Existen dos tipos de soluciones VPN: IPSec VPN o SSL VPN. Una IPSec VPN asume que los dos endpoints, site-to-site o client-to-site, están conectados a través de una conexión de red virtual.
Con una IPSec VPN, los usuarios teóricamente tienen acceso a todos los recursos de la red. Una SSL VPN establece una conexión encriptada desde un browser hacia la aplicación deseada o conjunto de aplicaciones basadas en la credencial de un usuario. Este método de acceso permite que el usuario se "loguee" en el sistema pero con un control de qué aplicaciones están disponibles teniendo en cuenta el nivel de confianza del endpoint.

Site-to-Site VPN

Esta solución de VPN supone una comunicación de dispositivo a dispositivo con toda la información entre ellos protegida mediante la encriptación y un túnel autenticado. Con una VPN site-to-site, todos los usuarios mantienen una comunicación segura con el destino, la cual es más segura utilizando IPSec VPN.

Remote Access VPN

Esta solución VPN es típicamente implementada para los usuarios remotos como los teleworkers, partners de negocios, proveedores y otros usuarios remotos que requieran de acceso a los recursos de la red. Dependiendo de lo que se necesite, IPSec o SSL VPN pueden brindar un acceso remoto VPN. Como SSL VPN no necesita implementación, instalación o confi-





VXL es reconocida como la mejor opción en cliente delgado en cuanto a precio y beneficio. Con sus nuevos modelos VXL ahora ofrece el rango más amplio en la Industria. Junto con su garantía de tres años y una cadena de soporte a nivel mundial puede comprar los productos ***VXL*** ¡con confianza!

La Solución Thin-Client de Mayor Costo-Beneficio



Itona "Diseñado para Citrix":

- Serie Itona TC45xx & TC 46xx inalámbrico
- Suite de clientes instalado para los productos Citrix
- Funcionalidad completa para el usuario de Citrix al precio más bajo
- Procesador de 1Ghz VIA C7 el chipset más avanzado en la industria
- Opción de Linux, Windows CE o XPe
- Rebate instantáneo de US$20 para usuarios Citrix



Desktop Integrado Itona:

- La nueva solución integrada TI54xx
- Pantalla de 17" LCD
- LAN inalámbrico interno & 10/100 Ethernet
- Opción de Linux, Windows CE o Xpe
- La opción integrada de mejor precio en el mercado



Cliente Delgado Itona Laptop:

- La nueva serie en formato laptop TL37xx
- LAN inalámbrico interno
- Puerto PCMCIA para tarjeta celular opcional
- Opción de Linux o Windows Xpe
- El verdadero cliente delgado móvil

Algo más: Todos los equipos VXL incluyen la licencia de XLmanage, el poderoso software de administración remota y son respaldados por medio de nuestra infraestructura global de soporte incluyendo el servicio de personalización de configuración para proyectos especiales.

Para mayor información contáctese con:



Distribuidor Mayorista Regional de Valor Agregado
Chile: +562/446-8462 | **Brasil:** +5511/6847-4984
Argentina: +5411/4328-3939
vxl@globalsoftware.com.ar



Itona el Cliente Delgado Desktop Líder del Mercado

- Sistemas Operativos Linux, MS Windows CE y Xpe
- Totalmente silencioso, diseño sin ventilador y sin partes con movimiento
- Gráfica de 32 bits capaz de resolución hasta 1600 x 1200
- Gráficas integradas "trident blade 3D"
- Opción de 10/100 Ethernet y adaptadores de LAN inalámbricos
- Lector de "Smart Card" opcional
- 4 x Puertos USB 2.0, serial, paralelo y audio
- Emulaciones incluyen Citrix ICA, RDP, VNC & Unix/IBM

guración de software en la máquina del usuario, es una atractiva solución para los empleados y los clientes. SSL VPNS son, además, particularmente efectivas a la hora de conectar a los recursos internos de la empresa con los partners de negocios o con los clientes donde la instalación del software en las máquinas individuales es sumamente impráctico.

Antivirus

Al integrar el antivirus de Kaspersky Lab, el appliance de seguridad integrada de Juniper puede proteger el tráfico de Web, los e-mail y los Web mails de los archivos con virus, gusanos, backdoors, Troyanos y malware.

Web Filtering

Todo el contenido de Internet que es leído, enviado o recibido conlleva riesgos inherentes. El acceso de los empleados a Internet continúa incrementando el número de peligros potenciales que podrían impactar negativamente en cuatro formas diferentes:

• **Riesgos en la seguridad:** Virus, spyware y otros tipos de malware pueden entrar en la red de una compañía a través de servicios de webmail, la descarga de archivos, el uso indebido de mensajería instantánea, aplicaciones P2P y el acceso a sitios no relacionados con el trabajo.

• **Riesgos legales:** Contenidos inapropiados pueden derivar en asuntos complejos de discriminación u hostigamiento sexual, religioso o étnico. Además, la descarga y distribución de contenidos ilegales a través de la red corporativa puede presentar problemas legales para la compañía.

• **Riesgos de productividad:** Las tentaciones que generan los sitios no relacionados con el trabajo son infinitas. Sólo 20 minutos de navegación "recreacional" pueden costarle a una compañía con 500 empleados más de 8 mil dólares por semana.

• **Riesgos en la red:** Un empleado puede hacer colapsar la red simplemente al ingresar a un sitio web maligno. Otras actividades como la navegación "recreacional" o la descarga de archivos en mp3 congestionan la red, reduciendo su performance, afectando de forma negativa los negocios de la empresa.

Para prevenir este tipo de amenazas, Juniper Networks ofrece dos métodos de protección a través de filtros web integrados y redirigidos.

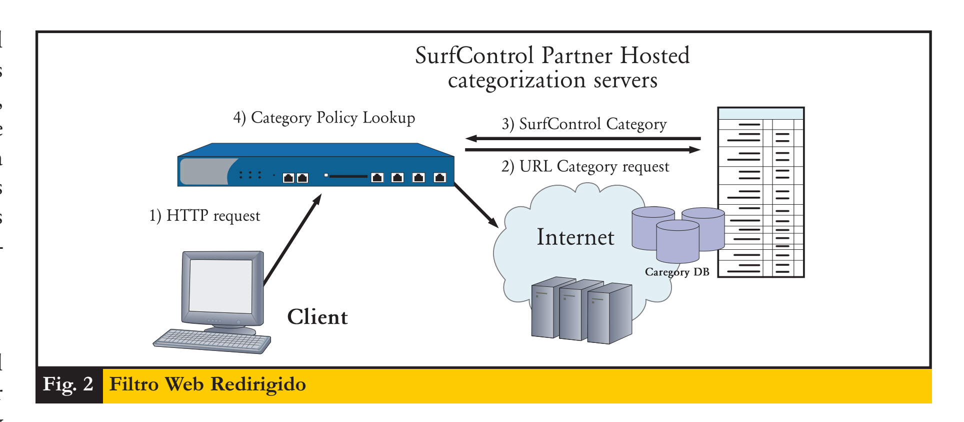


Fig. 2 Filtro Web Redirigido

Filtro Web Integrado

SurfControl es la herramienta de filtro web integrado que les permite a la empresas definir políticas de acceso a la Red a través del Firewall, utilizando ScreenOS webGUI, o bien mediante el acceso a la base de datos de URLs de SurfControl que incluye más de 13 millones de sites en 54 categorías diferentes.

1. El cliente inicia una solicitud de URL http.
2. El Firewall intercepta el pedido y chequea el cache del dispositivo para ir en busca de la URL. Si la URL no está en el cache, es enviada al servidor de SurfControl (hosteado por un socio de SurfControl).
3. El servidor responde enviando la categoría a la cual pertenece la URL solicitada, como por ejemplo, "Armas" o "Deportes".
4. El Firewall compara la categoría con los parámetros ingresados por el administrador y permite o bloquea el acceso al site, o bien redirecciona el tráfico a una página interna.
5. En caso de que la URL esté permitida, se garantiza su acceso vía http.

Filtro Web Redirigido

El Filtro Web Redirigido reúne los pedidos de acceso a la Red del firewall y los envía a un filtro en un servidor web externo para reforzar las políticas de filtrado de la organización. Con una solución de redireccionamiento, el cliente instala y administra la aplicación desde SurfControl o Websense.

1. El cliente inicia una solicitud URL http.
2. El Firewall intercepta el pedido y lo envía al servidor del filtro URL de SurfControl/Websense (instalado a pedido del cliente).
3. El filtro web responde según la política establecida para la URL, de acorde a la categoría, como "Armas" o "Deportes" y permite, niega o redirige la solicitud a una página interna.
4. En caso de que la solicitud sea aprobada, el acceso http queda garantizado.

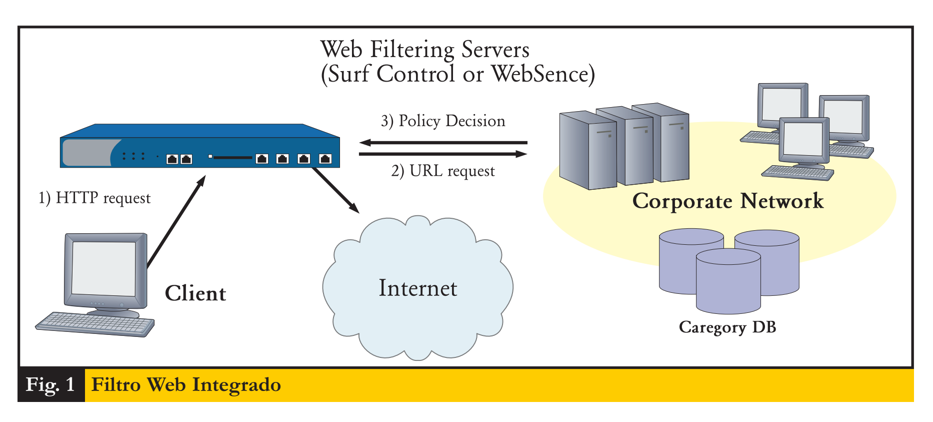


Fig. 1 Filtro Web Integrado

Anti-Spam

Para disminuir el número de correos no deseados y los potenciales ataques que acarrean, Juniper Networks se ha asociado con Symantec Corporation para ofrecer una solución Anti-Spam ideal para PyMEs. Instalado en el FW/VPN gateway, el motor Anti-Spam actúa como la primera línea de defensa, filtrando e-mails de conocidos spammers y ohishers. Cuando un correo malicioso es recibido, es bloqueado o marcado para que el servidor de correo lleve adelante las acciones correspondientes.

Consideraciones Adicionales sobre Layered Security

Una Layered Security Solution no puede ser verdaderamente efectiva si no es capaz de manejar el tráfico de la red, si es difícil de desplegar y/o de administrar, o si es incapaz de mantenerse confiable las 24 horas del día, los 7 días de la semana, los 365 días del año.

La solución de seguridad por capas de Juniper asegura los recursos de la red y los protege al proveer la habilidad de:

• Administrar las conexiones tanto a un VPN como Firewall a altas velocidades.
• Manejar los picos de tráfico generados tanto por el negocio como por ataques.
• Asegurar aplicaciones complejas como VoIP y streaming media.
• Integrarse con la red actual sin la necesidad de realizar importantes modificaciones.
• Facilitar la conectividad WAN.
• Operar de forma eficiente y confiable 24x7x365. ●

Tercera nota de la Serie .NET

Windows Communication Foundation

Gabriela Marina Giles
Microsoft .NET Senior Trainer
Presidenta de Desarrollador@s
Grupo de usuarios
de Tecnologías .NET

Descripción, Creación, Publicación y Utilización

Serie .NETNota #3

1) .NET Framework 3.0
WPF e Interfaces de Usuarios.

2) Programación de aplicaciones con AXML.

3) Descripción, Creación, Publicación y Utilización de Servicios con Windows Communication Foundation.

4) Windows Workflow Foundation
Fundamentos y Creación de Aplicaciones con funcionalidad de workflow.

WCF es un modelo de programación unificado que podemos utilizar para construir sistemas distribuidos, se basa en varias tecnologías actuales como Remoting, Web Services, Enterprise Services, Message Queue entre otras. Microsoft tomó lo más importante de cada una de esas tecnologías y lo combinó en una sola formando WFC, permitiendo a los desarrolladores de sistemas distribuidos utilizar esos conocimientos.

Windows Communication Foundation

WFC nos provee un conjunto de herramientas para simplificar el desarrollo de sistemas orientados a servicios. Este componente integra muchas tecnologías existentes como NET Remoting, MSMQ, Web Services, Enterprise services y Web Services Enhacements (WSE). WCF es una arquitectura basada en Web Services y utiliza estándares establecidos como SOAP, XML, HTTP, etc. Los servicios de WPF utilizan SOAP cuyo contenido es XML y pueden utilizar HTTP, TCP u otro mecanismo de transporte.
Existe una separación entre el transporte y el código, de esta manera soporta distintos métodos de comunicación haciendo más simple el desarrollo de sistemas orientados a servicios. Los servicios utilizan "mensajes" y canales como vía de comunicación. La estructura de un mensaje está compuesto por un sobre que contiene dos partes principales: encabezado y cuerpo. Los mensajes están envueltos en un sobre SOAP y representados como XML (figura 1).

Fig.1

WCF se compone de capas:
Contratos: Esta capa describe las operaciones, comportamiento, canales de comunicación y restricciones del servicio (Data Contract, Message Contract, Service Contract, Policy y Binding).

```
[ServiceContract()]
public interface IMyService
{
    [OperationContract]
    string MyOperation1(string myValue1);
    [OperationContract]
    string MyOperation2(DataContract1 dataContractValue);
}
```

Tabla.1

```
<public class MyService : IMyService
{
    public string MyOperation1(string myValue1)
    {
        return "Hello: " + myValue1;
    }
    public string MyOperation2(DataContract1 dataContractValue)
    {
        return "Hello: " + dataContractValue.FirstName;
    }
}
```

Tabla.2

Ejecución del servicio: Describe el comportamiento del servicio en ejecución, opera en el cuerpo del mensaje recibido.
Mensajería: Compuesta por los canales de comunicaciones, trabaja en la cabecera y el cuerpo del mensaje.
Hosting y Activación: Define las formas de ejecutar y activar un servicio. Por ejemplo Servicios de Windows, COM+ como servicios de WCF, EXE o IIS.
Un servicio WCF expone una colección de Endpoints o puntos de entradas representados por la clase ServiceEndpoint que se utilizará de acuerdo al tipo de canal de comunicación utilizada. Un EndPoint contiene una *Dirección* (**A**ddress), un *Enlace* (**B**inding) y un *Contrato* (**C**ontract). Para poder trabajar con WCF debemos bajar del sitio de descarga de Microsoft el Framework 3.0 y sus extensiones correspondientes. Desde Visual Studio .Net 2005 en las plantillas de proyectos, podemos seleccionar, por ejemplo, "crear nuevo sitio Web WCF Service" o "WCF Service". En el proyecto trabajaremos con la clase "Service.cs".
En la tabla 1 se declara el **"Service Contract"** que describe las operaciones que provee un servicio. Convierte los métodos de la interfaz de un servicio en una descripción de plataforma independiente (WSDL) y define el patrón de mensajes utilizado en el servicio.
Entonces el atributo **[ServiceContract]** contiene la definición del servicio y el atributo **[OperationContract]** define cuáles son las operaciones que puede llevar a cabo el servicio.
El código de la tabla 2 representa la implementación de los métodos de la interfaz.
En el último ejemplo de código (ver tabla 3) el atributo **Data Contract** describe la estructura de datos que es manejada por las funciones del servicio y **[DataMember]** define los atributos de ésta.

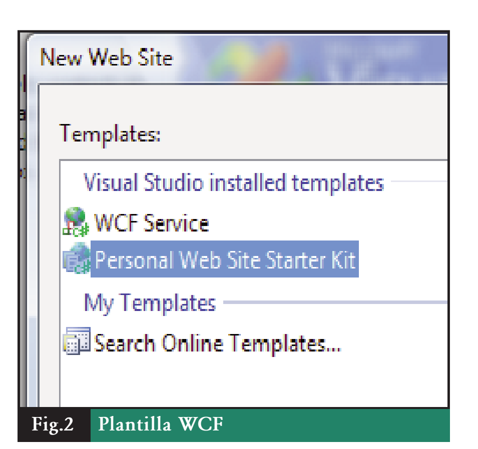


Fig.2 Plantilla WCF

En esta sección:
• Se define el tipo de estructura que intercambian los mensajes.
• Se describe el formato de la información pasada desde o hacia la función.
• Se define cómo serializar y deserializar los tipos de datos.
• Se convierte el tipo de datos en un XML Schema Definition (XSD).

Implementación

Para la implementación del Servicio se indica cómo se realizará el **Hosting**, para ello se utilizará la clase **ServiceHost**, que se encargará del alojamiento de nuestro servicio, al igual que lo hacía IIS con nuestros Servicios Web XML.
El Servicio debe estar alojarlo en un proceso o aplicación para poder ser utilizado, WCF nos proporciona la infraestructura de alojamiento necesaria. Además de especificar el tipo de servicio, también se puede especificar la dirección base para los diferentes transportes que se quieran utilizar.
El **consumidor del servicio** (Cliente) es una aplicación que debe conocer la Dirección (URI: http://localhost:8080/miService/), el Contrato y el Binding de un servicio para poder comunicarse e interactuar con el.
El intercambio de información (Datos) entre el cliente y el servicio se realiza por medio de Mensajes. Para conocer las capacidades y los requerimientos necesarios para poder interactuar con el servicio se utilizan las siguientes especificaciones:
• **XML Schema (XSD):** Describe estructuras complejas que se transfieren en los mensajes.
• **Web Services Description Language (WSDL):** Describe qué hace el servicio, cómo acceder a él y dónde encontrarlo.

Windows Application (WPF)
WCF Service Library
Console Application
Device Application
ASP.NET Web Service Application

Fig.3 Plantillas de proyectos

```
[DataContract]
public class DataContract1
{
    string firstName;
    string lastName;

    [DataMember]
    public string FirstName
    {
        get { return firstName;}
        set { firstName = value;}
    }
    [DataMember]
    public string LastName
    {
        get { return lastName;}
        set { lastName = value;}
    }
}
```

Tabla.3

• **WS-MetaDataExchange (WS-MEX):** Protocolo de acceso para solicitar la descripción del servicio.
• **WS-Policy:** Es usado para describir y aplicar políticas del servicio (Seguridad, Sesión, Disponibilidad).
Otros estándares de Web Service soportados:
• **WS-* architecture:** WS-Addressing, WS-AtomicTransaction, WS-ReliableMessaging, WS-Policy, WS-Security, WS-Trust, WS-Secure Conversation, WS-Coordination, WS-Policy, and MTOM.

WCF nos permite la creación, configuración e implementación de un Sistema Distribuido de forma sencilla mejorando la seguridad, performance e interoperabilidad. De esta forma, el desarrollo de sistemas orientados a servicios deja de ser una tarea compleja. ●

Links de Interés

•Visión Global de Arquitectura de Windows Communication Foundation: http://www.microsoft.com/spanish/msdn/articulos
•Windows Communication Foundation Downloads: http://msdn2.microsoft.com/en-us/netframework
•.NET Framework 3.0 Virtual Labs: http://msdn2.microsoft.com/en-us/virtuallabs/aa740389.aspx
•http://wcf.netfx3.com/

Nueva alianza entre Transistemas y Aranda Software



Con el objetivo de ofrecer una mayor cantidad de soluciones de gestión IT de alta calidad y eficaces para el desempeño de las organizaciones del cono sur, la empresa argentina Transistemas es ahora socio de negocios de Aranda Software. La alianza entre estas dos empresas consiste en brindar de manera coordinada los productos y servicios de Aranda además del acompañamiento a los clientes en su implementación. La compañía argentina se encargará de distribuir y asesorar a los usuarios en la adquisición y uso de las herramientas de gestión desarrolladas por Aranda.

De acuerdo con Matías Grandamarina, Coordinador de Marketing de Transistemas, "los clientes no sólo obtendrán las soluciones de software de Aranda, sino que les brindaremos los servicios profesionales y de mantenimiento asociados a las mismas".

Con 30 años de presencia en Argentina, Transistemas S.A. es una reconocida empresa proveedora de soluciones informáticas, de networking y de comunicaciones a organizaciones de todo tipo y tamaño en cualquier campo de la industria, no sólo en ese país sino en Chile, Ecuador, Perú, Uruguay, Bolivia, Paraguay y Brasil.

Aranda Software por su parte, es una empresa con presencia en Latinoamérica que desarrolla soluciones de gestión de activos, inventario informático, administración de infraestructura IT, seguridad informática, soluciones de soporte técnico, entre otras.

Con esta alianza, las organizaciones en Argentina ahora cuentan con mayor respaldo para adquirir soluciones informáticas que se ajusten a sus necesidades y a su presupuesto y así, lograr optimizar su gestión de recursos IT. ●

IronPort en manos de Cisco

Finalmente Cisco completó la compra de la empresa privada IronPort Systems, proveedora de productos de email y seguridad web que brindan protección contra spam, spyware, phishing y otras amenazas, por $830 millones de dólares en efectivo y en acciones.

Los productos y la tecnología de IronPort le permitirán a Cisco extender su estrategia de Red Autodefensiva (Self-Defending Network), que incluirá capacidades de Inspección de tráfico amplio, asegurando un nuevo enfoque que combina una gran profundidad en el nivel de seguridad de la red con una mayor variedad de capacidades para inspeccionar el tráfico de email, de web y de la mensajería instantánea

La visión de Cisco para una Red autodefensiva es incorporar protección dentro de la infraestructura entera de la red (junto con su portafolio de soluciones de routing y switching) y extender dicha protección desde la red (al nivel de paquete de datos) hacia las aplicaciones y el contenido. El agregado de la tecnología de seguridad de contenidos de IronPort le da a Cisco la posibilidad de proporcionar Inspección extendida de tráfico (Wide Traffic Inspection) que integra a la red y al análisis de contenido, para así frenar a las amenazas más sofisticadas y proteger a los protocolos de aplicaciones, los puntos finales y la red en sí mismos. ●

Sistema de comunicaciones empresariales Easy IP

D-Link LatinAmérica, anunció la disponibilidad en el mercado latinoamericano de su solución empresarial Easy IP, un nuevo Sistema de Comunicaciones IP para empresas.

El sistema Easy IP está compuesto por soluciones IP convergentes que permiten otorgar una solución integral a las empresas y sus necesidades actuales de comunicación de datos, voz y video. Este nuevo sistema de comunicación está compuesto -en una primera etapa- por el lanzamiento de la línea de soluciones de Telefonía IP especialmente diseñada para pequeñas y medianas empresas.

La solución central se basa en telefonía IP y se destaca la IP Private Branch Exchange (PBX), la cual permite que los empleados puedan comunicarse tanto al interior como al exterior de la compañía, mediante la convergencia entre la red de voz y la comunicación de datos. El principal beneficio de este tipo de comunicación de VoIP es que permite un gran ahorro en las empresas, sobre todo de los servicios de voz tradicional. ●



SSL VPNs vs. IPSec

Cuál es mejor, SSL o IPSec VPNs? La respuesta depende en lo que se considere como "mejor": a los usuarios les gusta SSL VPNs por su fácil uso aunque IPSec VPNs es atractiva por su seguridad.

Una encuesta realizada por la empresa Infonetic a 250 pequeñas, medianas y grandes empresas, reveló que los usuarios le dan el mayor puntaje en costo y complejidad a IPSec mientras que los usuarios de SSL VPN tienen sus reservas en cuanto a la seguridad y la protección.

Además, hay buenas noticias para Cisco: ellos se llevaron la mayor puntuación como vendor, quedando primeros en todas las categorías (a excepción del precio y de la relación precio - performance). Finalmente, el 69 por ciento de las organizaciones consultadas dijeron que planean implementar una fuerte autenticación para los usuarios de VPN para abril de 2009. ●

FOTO: http://www.sxc.hu/ - Craig Jewelr


Ferozo
Panel de Control de Hosting



BREVES



Novell premiado

Las soluciones de gestión empresarial de Novell ganaron en cinco categorías en los Premios Mundiales 2007 Global Product Excellence Customer Trust (Confianza de los consumidores en la excelencia del producto) de Info Security Products Guide, una publicación de Silicon Valley Communications y la publicación líder en el mundo sobre productos y tecnologías relacionados con la seguridad. Los ganadores de cada categoría se eligieron sobre la base de los votos de más de 18.000 consumidores finales y potenciales clientes de todo el mundo, a quienes se les pidió que eligieran los productos en los que más confiaban para proteger sus recursos digitales.

Estas son las soluciones de gestión de identidades, seguridad y recursos de Novell que ganaron premios en las siguientes categorías:

- **Novell® Identity Manager 3.5** por Excelencia en Gestión de Identidades.
- **Novell Access Manager™** por Excelencia en Gestión de Acceso.
- **Sentinel™ 6 de Novell** por Excelencia en Gestión de Seguridad.
- **Novell ZENworks® 7.5 Asset Management** por Excelencia en Gestión de Activos.
- **Novell ZENworks 7 Patch Management** por Excelencia en Gestión de Parches.

Red Hat está creciendo

Luego del cierre del primer trimestre se conoció que los ingresos totales de Red Hat ascendieron a $118,9 millones de dólares, lo que representa un aumento del 42 por ciento respecto del mismo trimestre del ejercicio anterior y un 7 por ciento respecto del trimestre anterior. Además, anunciaron que los ingresos por suscripción alcanzaron los $103 millones de dólares con un aumento interanual del 44 por ciento.

El resultado neto del trimestre fue de $16,2 millones de dólares, o de $0,08 dólares por acción diluida, en comparación con los $13,8 millones de dólares o los 0,07 dólares por acción diluida del mismo trimestre del ejercicio anterior.

Otros aspectos sobresalientes del trimestre fue el tercer Summit anual para clientes, socios y la comunidad que Red Hat llevó a cabo, el lanzamiento de la versión 5 de su sistema operativo insignia Red Hat Enterprise Linux y la práctica por primera vez de la estrategia de Arquitecturas Orientadas a los Servicios (SOA), estableciendo ediciones para desarrolladores y de clase empresarial del conjunto de soluciones Jboss.

Para más información visite: *http://investors.redhat.com*

Uds. Preguntan y nosotros respondemos

Dado la gran cantidad de preguntas, dudas e inquietudes que nos han hecho llegar nuestros lectores, decidimos compartirlas con todos e inaugurar una nueva sección de consultas. Nuestra propuesta es que nos envíen sus preguntas a **redaccion@nexweb.com.ar** y que luego nuestros especialistas les puedan dar su opinión y su punto de vista sobre los diferentes temas que abarca la revista.

De esta forma lograremos mantener una comunicación más fluida, conocer cuáles son sus inquietudes, qué temas son los de mayor interés y en qué puntos deberemos hacer un especial hincapié.

Los invitamos a que nos envíen sus preguntas a **redaccion@nexweb.com.ar** en donde mes a mes iremos respondiendo todas las consultas que vayan surgiendo.

¡No dejen de escribirnos!

III Jornadas openXpertya

Se llevaron a cabo en la Ciudad de Buenos Aires las Terceras Jornadas Funcionales openXpertya de Latinoamérica. El evento tuvo lugar en las instalaciones de CentralTECH entre los días 25 y 29 de Junio, cubriendo los aspectos de Consultoría Funcional, así como también las Técnicas de Parametrización ERP.

Participaron miembros de Empresas de Sistemas de Venezuela, Uruguay, Mendoza, Córdoba y Buenos Aires, entre otras.



Humor - *Por Severi*





Roberto Coceres, jugador del Nationwide Tour®. Campeonato Argentino de Profesionales, San Eliseo 2005.







Inscríbase en alguna de las clínicas y/o salidas que se realizarán en forma exclusiva para CEOS y CIOS.

www.mundodelsoporte.com



El Mundo del Soporte

A Member of SupportLand Network